HENRIK SAUGMANDSGAARD ØE
FŐTANÁCSNOK INDÍTVÁNYA
Az ismertetés napja: 2019. december 19.[1]

C-311/18. sz. ügy

Data Protection Commissioner
kontra
Facebook Ireland Ltd,
Maximillian Schrems,
a United States of America,
az Electronic Privacy Information Centre,
a BSA Business Software Alliance, Inc.,
a Digitaleurope részvételével

(a High Court [felsőbíróság, Írország] által benyújtott előzetes döntéshozatal iránti kérelem)

„Előzetes döntéshozatal – A természetes személyek védelme a személyes adatok kezelése vonatkozásában – (EU) 2016/679 rendelet – A 2. cikk (2) bekezdése – Hatály – Személyes adatok kereskedelmi célú továbbítása az Amerikai Egyesült Államokba – A továbbított adatok nemzetbiztonsági célú kezelése az Amerikai Egyesült Államok hatóságai által – 45. cikk – A harmadik országban biztosított védelmi szint megfelelőségének értékelése – 46. cikk – Az adatkezelő által nyújtott megfelelő garanciák – Általános adatvédelmi kikötések – Az 58. cikk (2) bekezdése – A felügyeleti hatóságok hatáskörei – 2010/87/EU határozat – Érvényesség – (EU) 2016/1250 végrehajtási határozat – »EU–USA adatvédelmi pajzs« – Érvényesség – Az Európai Unió Alapjogi Chartájának 7., 8. és 47. cikke”

Tartalomjegyzék

1 Eredeti nyelv: francia.

I. Bevezetés

1. A személyes adatok védelmének világszintű közös garanciái hiányában az ilyen adatok határokon átnyúló áramlásaihoz az a kockázat kapcsolódik, hogy megtörik az Európai Unión belül biztosított védelmi szint folytonossága. E kockázat korlátozása mellett az áramlások megkönnyítésére törekvő uniós jogalkotó három mechanizmust vezetett be, amely alapján a személyes adatok továbbíthatók az Unióból harmadik országba.

2. Először is ilyen továbbításra sor kerülhet egy olyan határozat alapján, amelyben az Európai Bizottság megállapítja, hogy a szóban forgó harmadik ország az oda továbbított adatok számára „megfelelő védelmi szintet” biztosít.[2] Másodsorban, ilyen határozat hiányában a továbbítás akkor engedélyezett, ha azt „megfelelő garanciák” övezik.[3] E garanciák az adatátadó és az adatátvevő között kötött, a Bizottság által elfogadott általános adatvédelmi kikötéseket tartalmazó szerződés formáját ölthetik. A GDPR harmadszor bizonyos eltéréseket határoz meg, amelyek többek között az érintett személy hozzájárulásán alapulnak, amelyek lehetővé teszik a harmadik országba történő továbbítást megfelelőségi határozat és a megfelelő garanciák hiányában is.[4]

2 Lásd a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendeletet (általános adatvédelmi rendelet) (HL 2016. L 119., 1. o.; helyesbítések: HL 2016. L 314., 72. o.; HL 2018. L 127., 2. o.; a továbbiakban: GDPR).

3 Lásd a GDPR 46. cikkét.

4 Lásd a GDPR 49. cikkét.

3. A High Court (felsőbíróság, Írország) által benyújtott előzetes döntéshozatal iránti kérelem a második ilyen mechanizmust érinti. Közelebbről a 2010/87/EU határozat [5] érvényességére vonatkozik, amely révén a Bizottság egyes továbbítás-kategóriák vonatkozásában általános szerződési feltételeket állapított meg, az Európai Unió Alapjogi Chartája (a továbbiakban: Charta) 7., 8. és 47. cikkére figyelemmel.

4. E kérelmet a Data Protection Commissioner (adatvédelmi biztos, Írország, a továbbiakban: DPC) és a Facebook Ireland Ltd, valamint Maximillian Schrems között folyó jogvitában terjesztették elő. Az utóbbi azzal kapcsolatos panaszt terjesztett a DPC elé, hogy a rá vonatkozó személyes adatokat a Facebook Ireland továbbította a Facebook Inc., vagyis az Amerikai Egyesült Államokban (a továbbiakban: Egyesült Államok) található anyavállalata részére. A DPC úgy véli, hogy e panasz elbírálása attól függ, hogy érvényes-e a 2010/87 határozat. Ebben az összefüggésben a kérdést előterjesztő bírósághoz fordult, felkérve azt, hogy intézzen kérdést a Bírósághoz.

5. Kiindulásként jelzem, hogy az előzetes döntéshozatalra előterjesztett kérdések vizsgálata álláspontom szerint nem tárt fel olyan körülményt, amely kihathat a 2010/87 határozat érvényességére.

6. Egyébként a kérdést előterjesztő bíróság kiemelt bizonyos kétségeket, amelyek lényegében az Egyesült Államok által biztosított védelmi szint megfelelőségét érintik azon beavatkozásokra figyelemmel, amelyeket az amerikai hírszerzési hatóságok tevékenysége eredményez azon személyek alapvető jogainak gyakorlására nézve, akiknek adatait e harmadik országba továbbították. E kétségek közvetve a Bizottság által ezzel kapcsolatban az (EU) 2016/1250 végrehajtási határozatban [6] végzett értékeléseket kérdőjelezik meg. Noha az alapeljárás elbírálása nem igényli a Bíróság részéről e kérdés eldöntését, és ezért azt javaslom neki, hogy ne tegye azt meg, másodlagosan ismertetem azokat az indokokat, amelyek miatt megkérdőjelezem e határozat érvényességét.

7. Elemzésem egészét az egyensúly keresése vezérli, egyrészt azon követelmény között, hogy „észszerű mértékű pragmatizmust tanúsítsunk annak érdekében, hogy együtt tudjunk működni a világ többi részével”, [7] másrészt pedig azon követelmény között, amely szerint érvényesítenünk kell az Unió és tagállamai jogrendjében, különösen a Chartában elismert alapvető értékeket.

5 A 2016. december 16-i (EU) 2016/2297 bizottsági végrehajtási határozattal (HL 2016. L 344., 100. o.) módosított, a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló, 2010. február 5-i bizottsági határozat (HL 2010. L 39., 5. o.; a továbbiakban: 2010/87 határozat).

6 A [95/46 irányelv] alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló, 2016. július 12-i bizottsági határozat (HL 2016. L 207., 1. o., a továbbiakban: az adatvédelmi pajzsról szóló határozat).

7 Lásd a korábbi európai adatvédelmi biztos, P. Hustinx beszédét: „Le droit de l’Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données”, 49. o., elérhető a következő internetcímen: https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_fr.pdf.

II. Jogi háttér

A. A 95/46/EK irányelv

8. A személyes adatok feldolgozása [helyesen: kezelése] vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK európai parlamenti és tanácsi irányelv[8] 3. cikkének (2) bekezdése a következőképpen rendelkezett:

„Az irányelv nem alkalmazandó [helyesen: nem alkalmazható] az alábbi személyesadat-feldolgozásokra [helyesen: személyesadat-kezelésekre]:

– a közösségi jog hatályán kívül eső tevékenységek, mint például az Európai Unióról szóló szerződés V. és VI. címében megállapítottak, valamint a közbiztonsággal, a védelemmel, a nemzetbiztonsággal (beleértve az ország gazdasági jólétét is, ha a feldolgozási [helyesen: az adatkezelési] művelet nemzetbiztonsági ügyre vonatkozik [helyesen: nemzetbiztonsági üggyel kapcsolatos]), továbbá a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási [helyesen: adatkezelési] műveletek,

[…]”

9. Ezen irányelv 13. cikkének (1) bekezdése a következőket tartalmazta:

„A tagállamok jogszabályokat fogadhatnak el a 6. cikk (1) bekezdésében, a 10. cikkben. a 11. cikk (1) bekezdésében, valamint a 12. és a 21. cikkben foglalt jogok és kötelezettségek körének korlátozására, amennyiben a korlátozás az alábbiak biztosításához szükséges:

a) nemzetbiztonság;

b) honvédelem;

c) közbiztonság;

d) bűncselekmények vagy a szabályozott foglalkozások etikai vétségeinek megelőzése, vizsgálata, felderítése és az ezekkel kapcsolatos eljárások lefolytatása;

e) valamely tagállam vagy az [Unió] fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket;

f) a c), d) és e) pontban említett esetekben esetlegesen a hatósági feladatok gyakorlásához kapcsolódó ellenőrzési, felügyeleti és szabályozási tevékenység;

g) az érintett védelme vagy mások jogainak és szabadságainak védelme.”

10. Az említett irányelv 25. cikke a következőket írta elő:

„(1) A tagállamoknak rendelkezniük kell arról, hogy a feldolgozásra [helyesen: kezelésre] kerülő vagy továbbítás után feldolgozásra [helyesen: kezelésre] szánt személyes adatok csak akkor továbbíthatók harmadik országba, ha – az ezen irányelv egyéb rendelkezései értelmében elfogadott nemzeti rendelkezéseknek való megfelelés sérelme nélkül – az adott harmadik ország megfelelő védelmi szintet tud biztosítani [helyesen: biztosít].

8 A 2003. szeptember 29-i 1882/2003/EK európai parlamenti és tanács irányelvvel módosított, 1995. október 24-i európai parlamenti és tanács irányelv (HL 1995. L 281., 31. o.; magyar nyelvű különkiadás: 13. fejezet, 15. kötet, 355. o. a továbbiakban: 95/46 irányelv).

(2) A harmadik ország által nyújtott védelem szintjének megfelelő mivoltát az adattovábbítási művelet vagy adattovábbítási műveletsorozat feltételeinek figyelembevételével kell értékelni; különös figyelmet kell fordítani az adatok jellegére, a tervezett adatfeldolgozási [helyesen: adatkezelési] művelet vagy műveletek céljára és időtartamára, a kiindulási és a célországra, az adott harmadik országban hatályos, általános és ágazati jogrendre, valamint az adott országban érvényesülő szakmai szabályokra és biztonsági intézkedésekre.

[…]

(6) A Bizottság a 31. cikk (2) bekezdésében említett eljárásnak megfelelően megállapíthatja, hogy a harmadik ország megfelelő védelmi szintet biztosít e cikk (2) bekezdése értelmében, az egyének magánéletének, jogainak és szabadságainak védelmére vonatkozó belföldi jog, vagy a vállalt nemzetközi kötelezettségek, különösen az (5) bekezdésben említett tárgyalások végeredménye alapján [helyesen: belföldi joga vagy az egyének magánéletének, alapvető jogainak és szabadságainak védelme érdekében, különösen az (5) bekezdésben említett tárgyalások végeredménye alapján vállalt nemzetközi kötelezettségei alapján].

A tagállamok megtesznek minden szükséges intézkedést a Bizottság határozatának teljesítésére.”

11. Ugyanezen irányelv 26. cikkének (2) és (4) bekezdése előírta:

„(2) Az (1) bekezdés sérelme nélkül a tagállamok engedélyezhetik a személyes adatok olyan harmadik országba irányuló továbbítását vagy továbbítássorozatát, amely a 25. cikk (2) bekezdése értelmében nem biztosít megfelelő szintű védelmet, amennyiben az adatkezelő megfelelő garanciákat teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelme, továbbá a kapcsolódó jogok gyakorlása tekintetében; ilyen garanciát jelenthetnek elsősorban a megfelelő szerződési feltételek.

[…]

(4) Amennyiben a Bizottság […] úgy dönt, hogy egyes általános szerződési feltételek megfelelő biztosítékot nyújtanak a (2) bekezdés értelmében, a tagállamok megteszik a szükséges intézkedéseket a Bizottság határozatának teljesítésére.”

12. A 95/46 irányelv 28. cikke (3) bekezdésének szövege a következő volt:

„A hatóságok különösen a következő jogosultságokkal rendelkeznek:

[…]

– tényleges beavatkozási jogosultságok, mint például a 20. cikknek megfelelően végzett adatfeldolgozási [helyesen: adatkezelési] műveletek megkezdése előtti véleményezés joga, e vélemények megfelelő közzétételének biztosítása, az adatok zárolásának, törlésének vagy megsemmisítésének elrendelése, az adatfeldolgozás [helyesen: adatkezelés] átmeneti vagy végleges tilalmának megállapítása, az adatkezelő figyelmeztetése vagy megrovása, illetve az ügy nemzeti parlament vagy más politikai intézmény elé terjesztése,

[…]”

B. A GDPR

13. A 94. cikkének (1) bekezdése alapján a GDPR 2018. május 25-i hatállyal felváltotta a 95/46 irányelvet, amely időponttól kezdve az említett rendeletet 99. cikke (2) bekezdésének megfelelően alkalmazni kell.

14. Az említett rendelet 2. cikkének (2) bekezdése a következőképpen rendelkezik:

„E rendelet nem alkalmazandó a személyes adatok kezelésére, ha azt:

a) az uniós jog hatályán kívül eső tevékenységek során végzik;

b) a tagállamok az EUSZ V. címe 2. fejezetének hatálya alá tartozó tevékenységek során végzik;

[…]

d) az illetékes hatóságok bűncselekmények megelőzése, nyomozása, felderítése, vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzik, ideértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését.”

15. Ugyanezen rendelet 4. cikkének 2. pontja szerint az „adatkezelés” a „személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közléstovábbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés”.

16. A GDPR 23. cikke szerint:

„(1) Az adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja a 12–22. cikkben és a 34. cikkben foglalt, valamint a 12–22. cikkben meghatározott jogokkal és kötelezettségekkel összhangban lévő rendelkezései tekintetében az 5. cikkben foglalt jogok és kötelezettségek hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint az alábbiak védelméhez szükséges és arányos intézkedés egy demokratikus társadalomban:

a) nemzetbiztonság;

b) honvédelem;

c) közbiztonság;

d) bűncselekmények megelőzése, nyomozása, felderítése és a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését;

e) az Unió vagy valamely tagállam egyéb fontos, általános közérdekű célkitűzései, különösen az Unió vagy valamely tagállam fontos gazdasági vagy pénzügyi érdeke […];

[…]

(2) Az (1) bekezdésben említett jogalkotási intézkedések adott esetben részletes rendelkezéseket tartalmaznak legalább:

a) az adatkezelés céljaira vagy az adatkezelés kategóriáira,

b) a személyes adatok kategóriáira,

c) a bevezetett korlátozások hatályára,

d) a visszaélésre, illetve a jogosulatlan hozzáférésre vagy továbbítás megakadályozását célzó garanciákra,

e) az adatkezelő meghatározására vagy az adatkezelők kategóriáinak meghatározására,

f) az adattárolás időtartamára, valamint az alkalmazandó garanciákra, figyelembe véve az adatkezelés vagy az adatkezelési kategóriák jellegét, hatályát és céljait,

g) az érintettek jogait és szabadságait érintő kockázatokra, és

h) az érintettek arra vonatkozó jogára, hogy tájékoztatást kapjanak a korlátozásról, kivéve, ha ez hátrányosan befolyásolhatja a korlátozás célját."

17. E rendelet „Az adattovábbításra vonatkozó általános elv" című 44. cikke a következőket mondja ki:

„Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból vagy nemzetközi szervezettől egy további harmadik országba vagy további nemzetközi szervezet részére történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, e rendelet egyéb rendelkezéseinek betartása mellett, ha az adatkezelő és az adatfeldolgozó teljesíti az e fejezetben rögzített feltételeket. E fejezet valamennyi rendelkezését alkalmazni kell annak biztosítása érdekében, hogy a természetes személyek számára e rendeletben garantált védelem szintje ne sérüljön."

18. Az említett rendelet „Adattovábbítás megfelelőségi határozat alapján" című 45. cikke szerint:

„(1) Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha a Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély.

(2) A védelmi szint megfelelőségének mérlegelése során a Bizottság különösen a következő tényezőket veszi figyelembe:

a) a jogállamiság, az emberi jogok és alapvető szabadságok tiszteletben tartása, a vonatkozó általános és ágazati jogszabályok, köztük a közbiztonságra, a védelemre, valamint a nemzetbiztonságra vonatkozó és a büntetőjogi rendelkezések, a közhatalmi szerveknek a személyes adatokhoz való hozzáférését szabályozó rendelkezések, valamint e jogszabályok végrehajtása, adatvédelmi szabályok, szakmai szabályok és biztonsági intézkedések, ideértve a személyes adatok másik harmadik ország vagy nemzetközi szervezet részére történő újbóli továbbítására vonatkozó azon szabályokat, amelyeknek az adott országban vagy nemzetközi szervezeten belül meg kell felelni; ítélkezési gyakorlat, továbbá az, hogy az érintettek, akiknek a személyes adatait továbbítják, rendelkeznek-e hatékonyan érvényesíthető – a hatékony közigazgatási és bírósági jogorvoslatot is magukban foglaló – jogokkal;

b) a szóban forgó harmadik országban létezik-e egy vagy több olyan független és hatékonyan működő felügyeleti hatóság – a szóban forgó nemzetközi szervezet pedig ilyen hatóság ellenőrzése alatt áll-e –, amely felelős az adatvédelmi szabályok betartásának biztosításáért és végrehajtásáért, rendelkezik többek között megfelelő kikényszerítési hatáskörrel, és felelős az érintettek részére történő, a jogaik gyakorlásával kapcsolatos segítségnyújtásért és tanácsadásért, valamint a tagállami felügyeleti hatóságokkal való együttműködésért; továbbá

c) a szóban forgó harmadik ország vagy nemzetközi szervezet nemzetközi kötelezettségei vagy egyéb, jogilag kötelező erejű egyezményekből vagy jogi eszközökből, valamint többoldalú vagy regionális rendszerekben való részvételéből eredő – különösen a személyes adatok védelmével kapcsolatos – kötelezettségei.

(3) A védelmi szint megfelelőségének értékelését követően a Bizottság végrehajtási jogi aktusok útján határozhat arról, hogy a harmadik ország, a harmadik ország valamely területe, illetve egy vagy több meghatározott ágazata, illetve valamely nemzetközi szervezet a (2) bekezdés értelmében biztosítja a megfelelő védelmi szintet. A végrehajtási jogi aktusban rendelkezni kell egy rendszeres, legalább négyévente elvégzendő felülvizsgálatra irányuló mechanizmusról, amely az adott harmadik országban vagy nemzetközi szervezetnél végbement valamennyi releváns fejleményt figyelembe vesz. […]

(4) A Bizottság folyamatosan figyelemmel kíséri a harmadik országokban és a nemzetközi szervezeteknél végbement azon fejleményeket, amelyek érinthetik az e cikk (3) bekezdése, valamint a 95/46/EK irányelv 25. cikkének (6) bekezdése alapján elfogadott határozatok végrehajtását.

(5) A Bizottság – a rendelkezésekre álló információk, különösen az e cikk (3) bekezdésében említett felülvizsgálat alapján – határoz arról, hogy a harmadik ország, a harmadik ország valamely területe vagy meghatározott ágazata, vagy valamely nemzetközi szervezet már nem biztosítja az e cikk (2) bekezdése értelmében vett megfelelő védelmi szintet, és a szükséges mértékben, az e cikk (3) bekezdésében említett korábbi határozatot végrehajtási jogi aktus útján, visszaható hatály nélkül hatályon kívül helyezi, módosítja vagy felfüggeszti. […]

(6) A Bizottság konzultációt kezdeményez a harmadik országgal vagy nemzetközi szervezettel az (5) bekezdés szerinti határozat meghozatalához vezető helyzet orvoslását illetően.

[…]

(9) A Bizottság által a 95/46/EK irányelv 25. cikkének (6) bekezdése alapján elfogadott határozatok mindaddig hatályban maradnak, amíg azokat az e cikk (3) vagy az (5) bekezdésével összhangban elfogadott bizottsági határozat nem módosítja, nem váltja fel vagy nem helyezi hatályon kívül.”

19. Ugyanezen rendelet „Megfelelő garanciák alapján történő adattovábbítások” című 46. cikke a következőképpen szól:

„(1) A 45. cikk (3) bekezdése szerinti határozat hiányában az adatkezelő vagy adatfeldolgozó csak abban az esetben továbbíthat személyes adatokat harmadik országba vagy nemzetközi szervezet részére, ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

(2) A felügyeleti hatóság külön engedélye nélkül az (1) bekezdés szerinti megfelelő garanciákat az alábbiak jelenthetik:

[…]

c) a Bizottság által a 93. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban elfogadott általános adatvédelmi kikötések;

[…]

(5) A valamely tagállam vagy felügyeleti hatóság által a 95/46/EK irányelv 26. cikkének (2) bekezdése alapján kiadott engedélyek hatályban maradnak mindaddig, amíg azokat szükség esetén a felügyeleti hatóság nem módosítja, nem váltja fel vagy nem helyezi hatályon kívül. A Bizottság által a 95/46/EK irányelv 26. cikkének (4) bekezdése alapján elfogadott határozatok mindaddig hatályban maradnak, amíg azokat szükség esetén az e cikk (2) bekezdésével összhangban elfogadott bizottsági határozat nem módosítja, nem váltja fel vagy nem helyezi hatályon kívül."

20. A GDPR 58. cikkének (2), (4) és (5) bekezdése értelmében:

„(2) A felügyeleti hatóság korrekciós hatáskörében eljárva:

a) figyelmezteti az adatkezelőt vagy az adatfeldolgozót, hogy egyes tervezett adatkezelési tevékenységei valószínűsíthetően sértik e rendelet rendelkezéseit;

b) elmarasztalja az adatkezelőt vagy az adatfeldolgozót, ha adatkezelési tevékenysége megsértette e rendelet rendelkezéseit;

c) utasítja az adatkezelőt vagy az adatfeldolgozót, hogy teljesítse az érintettnek az e rendelet szerinti jogai gyakorlására vonatkozó kérelmét;

d) utasítja az adatkezelőt vagy az adatfeldolgozót, hogy adatkezelési műveleteit – adott esetben meghatározott módon és meghatározott időn belül – hozza összhangba e rendelet rendelkezéseivel;

e) utasítja az adatkezelőt, hogy tájékoztassa az érintettet az adatvédelmi incidensről;

f) átmenetileg vagy véglegesen korlátozza az adatkezelést, ideértve az adatkezelés megtiltását is;

[…]

i) a 83. cikknek megfelelően közigazgatási bírságot szab ki, az adott eset körülményeitől függően az e bekezdésben említett intézkedéseken túlmenően vagy azok helyett; és

j) elrendeli a harmadik országbeli címzett vagy nemzetközi szervezet felé irányuló adatáramlás felfüggesztését.

[…]

(4) Az e cikk alapján a felügyeleti hatóságra ruházott hatáskörök gyakorlására megfelelő garanciák mellett kerülhet sor, ideértve az uniós és a tagállami jogban a Chartával összhangban meghatározott hatékony bírósági jogorvoslatot és tisztességes eljárást is.

(5) A tagállamok jogszabályban előírják, hogy a felügyeleti hatóságuk hatáskörrel rendelkezik arra, hogy e rendelet megsértéséről tájékoztassa az igazságügyi hatóságokat, és adott esetben bírósági eljárást kezdeményezzen vagy abban más módon részt vegyen e rendelet rendelkezéseinek érvényre juttatása érdekében."

C. A 2010/87 határozat

21. A 95/46 irányelv 26. cikkének (4) bekezdése alapján a Bizottság három határozatot fogadott el, amelyekben megállapította, hogy az azokban szereplő általános szerződési feltételek megfelelő biztosítékot nyújtanak az egyének magánélethez való jogának, alapvető jogainak és szabadságjogainak védelmét, valamint a megfelelő jogok gyakorlását illetően (a továbbiakban: ÁSZF-határozatok).[9]

22. Ezek közé tartozik a 2010/87 határozat, amelynek 1. cikke szerint „[a] mellékletben szereplő általános szerződési feltételek megfelelő biztosítékot nyújtónak minősülnek, tekintettel az egyének magánélethez való jogának, alapvető jogainak és szabadságjogainak védelmére, valamint a [95/46] irányelv 26. cikkének (2) bekezdése által előírt megfelelő jogok gyakorlására”.

23. E határozat 3. cikke értelmében:

„E határozat alkalmazásában a következő fogalommeghatározásokat kell alkalmazni:

[…]

c) »adatátadó«: a személyes adatokat továbbító adatkezelő;

d) »adatátvevő«: egy harmadik országban letelepedett olyan feldolgozó, aki vállalja, hogy az adatátadó utasításaival és e határozat feltételeivel összhangban történt adattovábbítást követően átveszi az adatátadótól a személyes adatokat – annak nevében történő – adatfeldolgozás céljából, és aki nem tartozik egy harmadik ország – [95/46] irányelv 25. cikkének (1) bekezdése szerinti – megfelelő védelmet biztosító rendszerének hatálya alá;

[…]

f) »alkalmazandó adatvédelmi jog«: az egyének alapvető jogaik és szabadságjogaik, különösen – a személyes adatok feldolgozásával kapcsolatban – a magánélet tiszteletben tartásához való jogaik védelméről szóló, az adatátadó letelepedési helye szerinti tagállamban tevékenykedő adatkezelőre vonatkozó jogszabály;

[…]”

24. Eredeti változatában az említett határozat 4. cikkének (1) bekezdése a következőket írta elő:

„A [95/46] irányelv II., III., V. és VI. fejezete alapján elfogadott nemzeti rendelkezéseknek való megfelelés céljából tett intézkedésekre vonatkozó hatásköröket nem érintve, a tagállamok illetékes hatóságai a magánszemélyek – személyes adatainak feldolgozására tekintettel történő – védelme érdekében élhetnek azzal a jogukkal, hogy megtilthatják vagy felfüggeszthetik a harmadik országokba történő adattovábbítást olyan esetekben, ha:

a) megállapítják, hogy az adatátvevőre vagy a további feldolgozóra irányadó jog olyan követelményeket támaszt vele szemben, amelyek értelmében el kell térnie az alkalmazandó adatvédelmi jogtól, valamint amelyek – a [95/46] irányelv 13. cikkében foglalt, a demokratikus társadalomban

9 A [95/46] irányelv alapján a személyes adatok harmadik országokba irányuló továbbítására vonatkozó általános szerződési feltételekről szóló, 2001. június 15-i 2001/497/EK bizottsági határozat (HL 2001. L 181., 19. o.; magyar nyelvű különkiadás 13. fejezet, 26. kötet, 347. o.); a [2001/497] határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről szóló, 2004. december 27-i 2004/915/EK bizottsági határozat (HL 2004. L 385., 74. o.); valamint a 2010/87 határozat.

szükséges korlátozásokat – túllépik; és amennyiben ezek a követelmények vélhetően jelentős hátrányos hatással lesznek az alkalmazandó adatvédelmi jog és az általános szerződési feltételek által nyújtott garanciákra;

b) az illetékes hatóság megállapította, hogy az adatátvevő vagy a további feldolgozó nem tartotta be a mellékletben szereplő általános szerződési feltételeket; vagy

c) nagy a valószínűsége, hogy a mellékletben szereplő általános szerződési feltételeknek nem tesznek eleget vagy nem fognak eleget tenni, és az adattovábbítás folytatása súlyosan veszélyeztetné az érintetteket."

25. A 2010/87 határozat (EU) 2016/2297 végrehajtási határozat[10] általi módosításából következő jelenlegi változatának 4. cikke azt mondja ki, hogy „[h]a a tagállamok hatáskörrel rendelkező hatóságai oly módon gyakorolják a [95/46 irányelv] 28. cikkének (3) bekezdése alapján őket megillető jogköreiket, hogy ez – az egyéneknek a személyes adataik kezelése tekintetében történő védelme érdekében – harmadik országokba irányuló adatáramlás felfüggesztéséhez vagy végleges tilalmához vezet, az érintett tagállam haladéktalanul tájékoztatja erről a Bizottságot, amely továbbítja ezt a tájékoztatást a többi tagállamnak".

26. A 2010/87 határozat mellékletében több általános szerződési feltétel szerepel. Közelebbről az e mellékletben található „A kedvezményezett harmadik személyről szóló rendelkezés" című 3. általános szerződési feltétel az alábbiakat írja elő:

„(1) Az érintett az adatátadóval szemben – kedvezményezett harmadik személyként – érvényesítheti ezt az általános szerződési feltételt, a 4. általános szerződési feltétel b)–i) pontját, az 5. általános szerződési feltétel a)–e), valamint g)–j) pontját, a 6. általános szerződési feltétel (1) és (2) bekezdését, a 7. általános szerződési feltételt, a 8. általános szerződési feltétel (2) bekezdését, valamint a 9–12. általános szerződési feltételt.

(2) Az érintett az adatátvevővel szemben érvényesítheti ezt az általános szerződés feltételt, az 5. általános szerződési feltétel a)–e) és g) pontját, a 6. és 7. általános szerződési feltételt, a 8. általános szerződési feltétel (2) bekezdését, valamint a 9–12. általános szerződési feltételt azokban az esetekben, amikor az adatátadó vállalkozása ténylegesen vagy jogilag megszűnik létezni, feltéve hogy nincs olyan jogutód, amely az adatátadó valamennyi jogi kötelezettségét szerződéses vagy jogszabályi úton átvállalta, aminek eredményeként gyakorolja az adatátadó jogait és kötelezettségeit, amely esetben az érintett ezeket érvényesítheti e jogutóddal szemben.

[…]"

27. Az említett melléklet „Az adatátadó kötelezettségei" című 4. általános szerződési feltétele a következőképpen rendelkezik:

„Az adatátvevő elfogadja és garantálja, hogy:

a) a személyes adatok feldolgozása, ideértve magát az adattovábbítást is, megfelelt és továbbra is megfelel az alkalmazandó adatvédelmi jog vonatkozó hatályos rendelkezéseinek (és adott esetben erről értesítették az adatátadó letelepedési helye szerinti tagállam hatóságait), valamint nem sérti az adott állam vonatkozó rendelkezéseit;

10 A [95/46] irányelv alapján a személyes adatok harmadik országokba és harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló [2001/497] és [2010/87] határozatok módosításáról szóló, 2016. december 16-i bizottsági határozat (HL 2016. L 344., 100. o.).

b) ellátta és a személyes adatok feldolgozása során folyamatosan ellátja az adatátvevőt arra vonatkozó utasításokkal, hogy a továbbított személyes adatokat csak az adatátadó megbízásából és az alkalmazandó adatvédelmi joggal, továbbá az általános szerződési feltételekkel összhangban lehet feldolgozni;

c) az adatátvevő elegendő garanciával szolgál majd e szerződéshez csatolt 2. függelékben meghatározott technikai és szervezési biztonsági intézkedések tekintetében;

d) az alkalmazandó adatvédelmi jog követelményeinek értékelését követően a biztonsági intézkedések alkalmasak a személyes adatok véletlen vagy jogellenes megsemmisülése, illetve a véletlen elvesztés, megváltozás, adatok jogosulatlan közlése vagy az azokhoz történő jogosulatlan hozzáférés elleni védelemre, különösen azokban az esetekben, ahol az adatfeldolgozás része az adatok hálózaton történő továbbítása, valamint az adatfeldolgozás egyéb jogellenes formái elleni védelemre; továbbá azt, hogy ezek az intézkedések olyan szintű biztonságot nyújtanak, amely arányos a megvédendő adatok jellegével és az adatfeldolgozás kockázataival, tekintettel a mindenkori aktuális körülményekre és a végrehajtás költségeire;

e) gondoskodik a biztonsági intézkedések tiszteletben tartásáról;

f) amennyiben az adattovábbítás különleges adatkategóriákat érint, az érintettet az adattovábbítást megelőzően vagy – a lehető legrövidebb időn belül – az adattovábbítást követően tájékoztatják arról, hogy az adatokat egy olyan harmadik országba továbbítják, amely nem biztosítja a [95/46 irányelv] szerinti megfelelő mértékű védelmet;

g) továbbítja az adatvédelmi felügyeleti hatóság felé az adatátvevőtől és bármely további feldolgozótól az 5. általános szerződési feltétel b) pontja és a 8. általános szerződési feltétel (3) bekezdése értelmében átvett értesítést, amennyiben az adatátadó úgy dönt, hogy folytatja az adattovábbítást vagy megszünteti a felfüggesztést;

h) az érintettek kérésére rendelkezésükre bocsátja az általános szerződési feltételek egy példányát, a 2. függelék kivételével, és a biztonsági intézkedések összefoglaló leírását, valamint a további feldolgozásra vonatkozó – általános szerződési feltételekkel összhangban megkötendő – szerződések egy példányát, feltéve, hogy az általános szerződési feltételek vagy a szerződés nem tartalmaznak üzleti információt, amely esetben eltávolíthatja ezen üzleti információkat;

i) további feldolgozás esetén a feldolgozási tevékenységet a további feldolgozó a 11. általános szerződési feltétellel összhangban végzi a személyes adatok és az érintett jogainak legalább olyan szintű biztosítása mellett, mint amilyet általános szerződési feltétel alapján az adatátvevő biztosítana; és

j) biztosítja a 4. általános szerződési feltétel a)–i) pontjának való megfelelést.”

28. Az említett melléklet „Az adatátvevő kötelezettségei ([1])” című 5. általános szerződési feltétele a következőképpen rendelkezik:

„Az adatátvevő elfogadja és garantálja, hogy:

a) csak az átadó nevében, utasításaival és az általános szerződési feltételekkel összhangban dolgozza fel a személyes adatokat; amennyiben bármely oknál fogva nem képes megfelelni ezeknek a követelményeknek, haladéktalanul tájékoztatja erről az adatátadót, aki ez esetben jogosult felfüggeszteni az adattovábbítást és/vagy a szerződéstől elállni;

b) nincs tudomása arról, hogy a rá vonatkozó jogszabályok akadályoznák az adatátadótól kapott utasítások és a szerződésben vállalt kötelezettségek teljesítését – abban az esetben, ha a jogszabályok módosítása előreláthatóan jelentősen hátrányos hatással lenne az általános szerződési feltételekben rá vonatkozóan megállapított garanciákra és kötelezettségekre, mihelyt azonban tudomást szerez erről, azonnal értesíti a módosításról az adatátadót –, ebben az esetben az adatátadó jogosult felfüggeszteni az adattovábbítást és/vagy a szerződéstől elállni;

c) a továbbított személyes adatok feldolgozása előtt végrehajtotta a 2. függelékben meghatározott technikai és szervezési biztonsági intézkedéseket;

d) azonnal értesíti majd az adatátadót a következőkről:

   i. ellenkező értelmű tilalom – például egy bűnügyi nyomozás titkosságának megőrzése érdekében fennálló büntetőjogi tilalom – hiányában a bűnüldöző szervek jogilag kötelező erejű felhívása a személyes adatok közlésére;

   ii. bármilyen véletlen vagy jogosulatlan hozzáférés; és

   iii. közvetlen az érintettek részéről érkező kérelem, erre adott válasz nélkül, kivéve, ha erre felhatalmazást kapott.

e) azonnal és szakszerűen reagál az adatátadótól érkező, az adattovábbítás tárgyát képező személyes adatok feldolgozására vonatkozó valamennyi kérdésre, és követi a felügyeleti hatóság adatfeldolgozásra vonatkozó javaslatait;

f) az adatátadó kérésére rendelkezésre bocsátja az adatfeldolgozó berendezéseket az általános szerződési feltételek hatálya alá eső feldolgozói tevékenységek ellenőrzése céljából, amelyet az adatátadó vagy a megfelelő szakképzettséggel rendelkező, az adatok bizalmas kezelésére kötelezett, az adatátadó által – adott esetben a felügyeleti hatóság beleegyezésével – kiválasztott, független szakértőkből álló testület végez;

[…]”

29. A 2010/87 rendelet mellékletében található 5. általános szerződési feltételben hivatkozott 1. lábjegyzet szerint:

„Az adatátvevőre vonatkozó nemzeti jogszabályok kötelező követelményei, amelyek nem lépnek túl azon, amire a [95/46] irányelv 13. cikkének (1) bekezdésében felsorolt érdekek valamelyike alapján egy demokratikus társadalomban szükség van; vagyis amennyiben ezek az érdekek olyan intézkedések alkalmazását írják elő, amelyek a nemzetbiztonsági, honvédelmi, közbiztonsági érdekek érvényesítését, a bűncselekmények megelőzését, a nyomozást, felderítését vagy üldözését, vagy – szabályozott szakmákban – etikai szabályok megsértését, az állam fontos gazdasági vagy pénzügyi érdekének védelmét, az érintett védelmét vagy mások jogainak vagy szabadságainak védelmét érintik, és nem ellentétesek az általános szerződési feltételekkel. Egy demokratikus társadalomban ezen elengedhetetlenül szükséges követelmények közé tartoznak többek között a nemzetközileg elfogadott szankciók, adóügyi követelmények, illetve a pénzmosás megelőzését szolgáló bejelentési követelmények.”

30. Az e mellékletben található, „Felelősség” című 6. általános szerződési feltétel szövege a következő:

„(1) A felek megállapodnak abban, hogy az érintett, aki a 3. vagy a 11. általános szerződési feltételben említett kötelezettségek egyik fél vagy a további felhasználó általi megsértésének következményeként kárt szenved, kártérítésre jogosult az adatátadótól.

(2) Amennyiben az érintett – az adatátvevőnek vagy az által megbízott további feldolgozónak a 3. vagy a 11. általános szerződési feltételben meghatározott kötelezettsége valamelyikének megszegéséből eredően – nem tudja érvényesíteni az (1) bekezdés szerinti kártérítési igényt az adatátadóval szemben azért, mert az adatátadó ténylegesen megszűnt, jogilag megszűnt létezni vagy fizetésképtelenné vált, az adatátvevő hozzájárul ahhoz, hogy az érintett vele szemben érvényesíthesse az adatátadóval szembeni kártérítési igényét, feltéve hogy nincs olyan jogutód, amely az adatátadó valamennyi jogi kötelezettségét szerződéses vagy jogszabályi úton átvállalta, amely esetben az érintett e jogutóddal szemben érvényesítheti jogait.

[…]”

31. Az említett melléklet „Közvetítés és joghatóság” című 7. általános szerződési feltétele a következőképpen rendelkezik:

„(1) Az adatátvevő elfogadja, hogy amennyiben az érintett érvényesíteni kívánja vele szemben a kedvezményezett harmadik személy jogait, és/vagy az általános szerződési feltételek alapján követeli a károk megtérítését, az adatátvevő elfogadja az érintett következő döntéseit:

a) a jogvitával közvetítés céljából egy független személyhez vagy – adott esetben – a felügyeleti hatósághoz fordul;

b) a jogvitával az adatátadó letelepedési helye szerinti tagállam bíróságához fordul.

(2) A felek megállapodnak abban, hogy az érintett választása nem érinti az érintett arra vonatkozó anyagi vagy eljárási jogait, hogy a nemzeti vagy nemzetközi jog egyéb rendelkezéseivel összhangban jogorvoslattal éljen.”

32. Az ugyanezen mellékletben található, „Irányadó jog” című 9. általános szerződési feltétel azt írja elő, hogy az általános szerződési feltételekre az adatátadó letelepedési helye szerinti tagállam joga az irányadó.

D. Az adatvédelmi pajzsról szóló határozat

33. A 95/46 határozat 25. cikkének (6) bekezdése alapján a Bizottság két egymást követő határozatot fogadott el, amelyek révén megállapította, hogy az Egyesült Államok megfelelő szintű védelmet biztosít az azon egyesült államokbeli vállalkozásokhoz továbbított személyes adatok tekintetében, amelyek egy öntanúsítási eljárás révén csatlakoznak az e határozatokban rögzített elvekhez.

34. A Bizottság először elfogadta az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő” elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló 2000/520/EK határozatot.[11] A 2015. október 6-i Schrems ítéletben[12] a Bíróság érvénytelennek nyilvánította e határozatot.

35. Ezen ítéletet követően a Bizottság másodszorra elfogadta az adatvédelmi pajzsról szóló határozatot:

36. E határozat 1. cikke a következőképpen rendelkezik:

„(1) A [95/46 irányelv] 25. cikke (2) bekezdésének alkalmazásában az Egyesült Államok megfelelő szintű védelmet biztosít az EU–USA adatvédelmi pajzs keretében az Unióból az egyesült államokbeli szervezetekhez továbbított személyes adatok tekintetében.

11 2000. július 26-i határozat, a [95/46] irányelv alapján (HL L 200. L 215., 7. o., a továbbiakban: „biztonságos kikötő” határozat).

12 C-362/14 (EU:C:2015:650, a továbbiakban: Schrems ítélet).

(2) Az EU–USA adatvédelmi pajzsot az Egyesült Államok Kereskedelmi minisztériuma által 2016. július 7-én kibocsátott, a II. mellékletben ismertetett elvek, valamint az I. és a III–VII. mellékletben felsorolt dokumentumokban foglalt hivatalos nyilatkozatok és kötelezettségvállalások alkotják.

(3) Az (1) bekezdés alkalmazásában a személyes adatok az EU–USA adatvédelmi pajzs keretében kerülnek továbbításra, amennyiben az Unióból egy olyan egyesült államokbeli szervezethez továbbítják azokat, amelyet – a II. mellékletben ismertetett elvek I. és III. szakaszának megfelelően – felvettek az »adatvédelmi pajzsban részt vevő szervezetek listájára«", amelyet az Egyesült Államok Kereskedelmi Minisztériuma vezet és a nyilvánosság számára hozzáférhetővé tesz."

37. E határozat „EU–USA adatvédelmi pajzs ombudsmani mechanizmus" című, az akkori Secretary of State (külügyminiszter, Egyesült Államok), John Kerry 2016. július 7-i leveléhez csatolt III. A. melléklet tartalmaz egy, a külügyminiszter által kinevezett „nemzetközi informatikai diplomáciai főkoordinátor" (a továbbiakban: ombudsman) előtt folyó új közvetítési eljárást ismertető feljegyzést.

38. A feljegyzés szerint ezt az eljárást „az [Unióból] az Egyesült Államokba az adatvédelmi pajzs keretében továbbított adatokhoz nemzetbiztonsági okokból történő hozzáférés iránti kérelmek kezelésének elősegítésére [vezették be], az általános szerződéses feltételeket (SCC-k), a kötelező erejű vállalati szabályokat (BCR-ek), az »eltéréseket« vagy »esetleges jövőbeli eltéréseket«, az Egyesült Államok vonatkozó jogszabályai és politikája szerinti bevezetett csatornákon keresztül, valamint az ilyen kérelmekre adott válaszokat.[helyesen: „azért {vezették be}, hogy elősegítsék az [Unió]ból az Egyesült Államokba az adatvédelmi pajzs, általános szerződési feltételek (SCC-k), kötelező erejű vállalati szabályok (BCR-ek), »eltérések« vagy »esetleges jövőbeli eltérések« keretében, az Egyesült Államok vonatkozó jogszabályai és politikája szerint bevezetett csatornákon keresztül továbbított adatokhoz nemzetbiztonsági okokból történő hozzáférés iránti kérelmek kezelését, valamint az ilyen kérelmekre adott válaszokat]"

III. Az alapeljárás, az előzetes döntéshozatala előterjesztett kérdések és a Bíróság előtti eljárás

39. M. Schrems, Ausztriában lakóhellyel rendelkező osztrák állampolgár a Facebook közösségi háló felhasználója. E szociális háló Unió területén lakó valamennyi felhasználójának a regisztráció során alá kell írnia egy szerződést az Egyesült Államokban letelepedett Facebook Inc. leányvállalatával, a Facebook Irelanddel. E felhasználók személyes adatait részben vagy egészben a Facebook Inc. Egyesült Államokban található szervereire továbbítják, és ott kezelik azokat.

40. 2013. június 25-én M. Schrems panaszt nyújtott be a DPC-hez, amelyben lényegében azt kérte, hogy tiltsa meg a Facebook Ireland számára a személyes adatai Egyesült Államokba való továbbítását. Azzal érvelt, hogy e harmadik ország hatályos joga és gyakorlata nem biztosít a területén tárolt személyes adatok számára elégséges védelmet a hatóságok által folytatott megfigyelési tevékenységekből következő beavatkozásokkal szemben. M. Schrems e tekintetben az Edward Snowden által az Egyesült Államok hírszerző szolgálatainak, és különösen a National Security Agency-nek (NSA) (Nemzetbiztonsági Ügynökség, Egyesült Államok) a tevékenységére vonatkozóan kiszivárogtatott információkra hivatkozott.

41. E panaszt elutasították, többek között azzal az indokkal, hogy az Egyesült Államokban biztosított védelem megfelelőségére vonatkozó minden kérdést a „biztonságos kikötő" határozattal összhangban kell vizsgálni. E határozatban a Bizottság megállapította, hogy e harmadik ország a területén található, az említett határozatban rögzített elvekhez csatlakozó vállalkozások részére továbbított személyes adatok tekintetében megfelelő védelmi szintet biztosít.

42. M. Schrems a panaszát elutasító határozattal szemben keresetet nyújtott be a High Court (felsőbíróság) előtt. E bíróság úgy ítélte meg, hogy bár M. Schrems formálisan nem kérdőjelezte meg a „biztonságos kikötő” határozat érvényességét, panasza valójában az e határozattal létrehozott rendszer jogszerűségét vitatja. E körülmények között az említett bíróság lényegében azzal kapcsolatban terjesztett kérdéseket a Bíróság elé, hogy a tagállam adatvédelemért felelős hatóságait (a továbbiakban: felügyeleti hatóságok), amennyiben valamely személy harmadik országba továbbított személyes adatainak kezelésével összefüggésben jogainak és szabadságainak védelmével kapcsolatos panaszt terjeszt eléjük, kötelezik-e az e harmadik ország által biztosított védelmi szint megfelelősége kapcsán a Bizottság által a 95/46 irányelv 25. cikkének (6) bekezdése alapján tett megállapítások, noha maga a panaszos is vitatja azokat.

43. Miután a Bíróság a Schrems ítélet 51. és 52. pontjában megállapította, hogy a megfelelőségi határozat addig kötelezi a felügyeleti hatóságokat, amíg nem állapítják meg annak érvénytelenségét, ezen ítélet 63. és 65. pontjában a következőket mondta ki:

„(63) […] [A]mennyiben valamely személy, akinek a személyes adatait olyan harmadik országba továbbították vagy továbbíthatják, amely a Bizottság által a 95/46 irányelv 25. cikkének (6) bekezdése alapján hozott határozat tárgyát képezi, e személyes adatok kezelése vonatkozásában kérelemmel fordul a nemzeti felügyelő hatósághoz jogainak vagy szabadságainak védelmével kapcsolatban, és e kérelem keretében – az alapügyhöz hasonlóan – e határozatnak a személyek magánélete, valamint alapvető jogai és szabadságai védelmével való összeegyeztethetőségét vitatja, e hatóság feladata, hogy kellő gondossággal megvizsgálja az említett kérelmet.

[…]

(65) [H]a az említett hatóság megalapozottnak ítéli meg [az e] személy által felhozott kifogásokat, ugyanezen hatóságnak – a 95/46 irányelvnek a Charta 8. cikke (3) bekezdésével összefüggésben értelmezett 28. cikke (3) bekezdése harmadik albekezdésének harmadik francia bekezdése alapján – lehetőséggel kell rendelkeznie ahhoz, hogy bírósági eljárást indítson. Ezzel összefüggésben a nemzeti jogalkotó feladata, hogy előírja azon jogorvoslati lehetőségeket, amelyek lehetővé teszik az érintett nemzeti felügyelő hatóság számára, hogy a nemzeti bíróságok előtt az általa megalapozottnak talált kifogásokra hivatkozzon annak érdekében, hogy amennyiben az utóbbiak osztják e hatóságnak a bizottsági határozat érvényessége tekintetében fennálló kétségeit, előzetes döntéshozatali eljárást kezdeményezhessenek e határozat érvényességének vizsgálata céljából.”

44. A Bíróság az említett ítéletben a „biztonságos kikötő” határozat érvényességét is megvizsgálta a Charta fényében értelmezett 95/46 irányelvből következő követelmények alapján. E vizsgálat eredményeként érvénytelennek nyilvánította az említett határozatot. [13]

45. A Schrems ítéletet követően a kérdést előterjesztő bíróság megsemmisítette azt a határozatot, amellyel a DPC elutasította M. Schrems panaszát, és azt vizsgálat céljából visszautalta a DPC elé. Az utóbbi vizsgálatot indított és felhívta M. Schrems-et arra, hogy fogalmazza át panaszát, figyelemmel a „biztonságos kikötő” határozat érvénytelenné nyilvánítására.

46. Ennek érdekében M. Schrems felhívta a Facebook Irelandet, hogy jelölje meg a Facebook közösségi háló felhasználói személyes adatainak az Unióból az Egyesült Államokba történő továbbításának jogalapjait. A Facebook Ireland, anélkül hogy megjelölte volna azokat a jogalapokat, amelyekre támaszkodik, egy közötte és a Facebook Inc. között kötött, 2015. november 20. óta alkalmazandó adattovábbítási és adatkezelési megállapodásra *(data transfer processing agreement)* utalt, valamint hivatkozott a 2010/87 határozatra.

13 Lásd: Schrems ítélet (106. pont).

47. Újrafogalmazott panaszában M. Schrems kifejti egyrészt, hogy az e megállapodásban szereplő kikötések nem felelnek meg a 2010/87 határozat mellékletében található általános szerződési feltételeknek. Másrészt M. Schrems előadja, hogy ezek az általános szerződési feltételek semmiképpen nem alapozhatják meg személyes adatainak az Egyesült Államokba való továbbítását. Ennek oka, hogy az amerikai jog azt írja elő a Facebook Inc. számára, hogy a Charta 7., 8. és 47. cikkében biztosított jogok gyakorlását akadályozó megfigyelési programok keretében a felhasználók személyes adatait bocsássa az olyan amerikai hatóságok rendelkezésére, mint az NSA és a Federal Bureau of Investigation (FBI) (Szövetségi Nyomozóiroda, Egyesült Államok). M. Schrems azt állítja, hogy semmilyen jogorvoslati lehetőség nem teszi lehetővé az érintettek számára, hogy érvényesítsék a magánélet tiszteletben tartásához és a személyes adatok védelméhez való jogukat. E körülmények között M. Schrems azt kéri, hogy a DPC a 2010/87 határozat 4. cikke alapján függessze fel ezt az adattovábbítást.

48. A Facebook Ireland a DPC vizsgálata keretében elismerte, hogy továbbra is továbbítja a Facebook közösségi háló Unióban lakóhellyel rendelkező felhasználói személyes adatait az Egyesült Államokba, valamint hogy e célból nagyrészt a 2010/87 határozat mellékletében szereplő általános szerződési feltételekre támaszkodik.

49. A DPC vizsgálata annak eldöntésére irányult, hogy egyrészt az Egyesült Államok az uniós polgárok személyes adatai számára megfelelő védelmi szintet biztosít-e, illetve másrészt, hogy nemleges esetben az ÁSZF-határozatok elegendő biztosítékot szolgáltatnak-e az uniós polgárok alapvető jogainak és szabadságainak védelmét illetően.

50. E tekintetben egy határozattervezetben *(draft decision)* a DPC ideiglenesen úgy ítélte meg, hogy az amerikai jog nem biztosít a Charta 47. cikkének értelmében vett hatékony jogorvoslati lehetőségeket azon uniós polgárok számára, akiknek személyes adatait az Egyesült Államokba továbbították, ahol fennáll annak veszélye, hogy az amerikai ügynökségek ezeket a Charta 7. és 8. cikkével összeegyeztethetetlen módon használják fel nemzetbiztonsági célokra. Az ÁSZF-határozatok mellékletében szereplő feltételekben előírt garanciák nem orvosolják e hiányosságot, mivel azok nem kötelezőek az Egyesült Államok hatóságaira vagy ügynökségeire nézve, és csak szerződéses jogokat ruháznak az érintettekre az adatátadóval és/vagy az adatátvevővel szemben.

51. E körülmények között a DPC úgy ítélte meg, hogy nem bírálhatja el M. Schrems panaszát anélkül, hogy a Bíróság ne vizsgálná meg az ÁSZF-határozatok érvényességét. A Schrems ítélet 65. pontjában előírtaknak megfelelően a DPC tehát arra irányuló eljárást indított a kérdést előterjesztő bíróság előtt, hogy az, amennyiben osztja a DPC kétségeit, intézzen előzetes döntéshozatal iránti kérelmet a Bírósághoz az említett határozatok érvényességét illetően.

52. Az Egyesült Államok kormánya, az Electronic Privacy Information Centre (EPIC), a Business Software Alliance (BSA) és a Digitaleurope számára engedélyezték a beavatkozást a kérdést előterjesztő bíróság előtt.

53. Annak eldöntése céljából, hogy egyetért-e az ÁSZF-határozatok érvényessége kapcsán a DPC által megfogalmazott kétségekkel, a High Court (felsőbíróság) megvizsgálta a jogvita felei által benyújtott bizonyítékokat és meghallgatta az általuk és a beavatkozók által ismertetett érveket. Közelebbről az Egyesült Államok jogának rendelkezései kapcsán szakértői véleményeket ismertettek. Az ír jogban a külföldi jogot olyan ténybeli elemnek tekintik, amelyet ugyanolyan módon kell bizonyítani, mint bármely más tényt. E bizonyítékok alapján a kérdést előterjesztő bíróság értékelte az Egyesült Államok jogának azon rendelkezéseit, amelyek lehetővé teszik a hatóságok és a kormányzati ügynökségek számára a megfigyelést, a két nyilvánosan elismert megfigyelési program (a PRISM és az Upstream) működését, az azon egyének számára nyitva álló jogorvoslati lehetőségeket, akiknek jogait a

megfigyelési intézkedések megsértették, valamint a rendszerszintű garanciákat és a felügyeleti mechanizmusokat. Az említett bíróság e mérlegelés eredményeit az előzetes döntéshozatalra utaló végzéshez csatolt, 2017. október 3-i ítéletben rögzítette (a továbbiakban: a High Court [felsőbíróság] 2017. október 3-i ítélete).

54. Ebben az ítéletben a kérdést előterjesztő bíróság – az amerikai hírszerző szolgálatok részére a külföldi közlések lehallgatását lehetővé tévő jogalapok között – hivatkozott a Foreign Intelligence Surveillance Act (FISA) (a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény) 702. cikkére, valamint az Executive Order 12333-ra (12333. sz. elnöki rendelet, a továbbiakban: EO 12333).

55. Az említett ítéletben rögzített megállapítások szerint a FISA 702. cikke lehetővé teszi az Attorney General (főügyész, Egyesült Államok) és a Director of National Intelligence (DNI) (nemzeti hírszerzési igazgató) részére, hogy külföldi hírszerzési információk szerzése céljából összesen egyéves időtartamra engedélyezze olyan személyek megfigyelését, akik nem amerikai állampolgárok és akik nem tartózkodnak tartósan az Egyesült Államokban (ún. nem amerikai személyek), amennyiben észszerűen feltételezhető, hogy azok az Egyesült Államok területén kívül tartózkodnak.[14] A FISA szerint a „külföldi hírszerzés” fogalma a kormánynak a terrorizmussal és a tömegpusztító fegyverek elterjedésével szembeni védekezési képességével, valamint az Egyesült Államok külügyeivel kapcsolatos információkat jelöli.[15]

56. Ezeket az éves engedélyeket, valamint a megfigyelendő személyekre irányultságot és a megszerzett információk kezelését („adattakarékosság”)[16] szabályozó eljárásokat jóvá kell hagynia a Foreign Intelligence Surveillance Courtnak (FISC) (külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság, Egyesült Államok). Míg a FISA más rendelkezésein alapuló „hagyományos” megfigyelés feltétele az, hogy megállapítsák egy olyan „valószínűsíthető indok” fennállását, amely alapján feltételezhető, hogy a megfigyelt személyek külföldi hatalomhoz tartoznak vagy annak ügynökei, addig a FISA 702. cikke alapján végzett megfigyelési tevékenységnek nem feltétele sem az ilyen „valószínűsíthető indok” megállapítása, sem az, hogy a FISC bizonyítsa a meghatározott személyekre irányultságot. Ezenkívül, továbbra is a kérdést előterjesztő bíróság megállapításai szerint, az adattakarékossági eljárások nem alkalmazandók az Egyesült Államokon kívül található nem amerikai személyekre.

57. A gyakorlatban a FISC által megadott engedélyt követően az NSA elküldi az egyesült államokbeli elektronikus hírközlési szolgáltatók részére a megcélzott személyhez kapcsolódó, „kiválasztási tényezőknek” nevezett keresési szempontokat (például telefonszámokat vagy e-mail-címeket) tartalmazó utasításokat. E szolgáltatók kötelesek az NSA kiválasztási tényezőinek megfelelő adatok továbbítására és kötelesek titkosan kezelni a részükre adott utasításokat. A szolgáltatók az NSA utasításának módosítására vagy hatályon helyezésére irányuló kérelmet terjeszthetnek a FISC elé. A FISC határozatával szemben fellebbezést lehet benyújtani a Foreign Intelligence Surveillance Court of Review-hoz (FISCR) (külföldi hírszerzési tevékenységek megfigyelésével foglalkozó fellebbviteli bíróság, Egyesült Államok).

58. A High Court (felsőbíróság) megállapította, hogy a FISA 702. cikke a jogalapja a PRISM és Upstream programoknak.

14 50 U. S. C. 1881 (a).

15 50 U. S. C. 1881 (e).

16 A kérdést előterjesztő bíróság megállapította, hogy a személyre irányultsággal kapcsolatos eljárások azt a módot érintik, amely szerint a végrehajtó hatalom eldönti, hogy észszerűen feltételezhető, hogy egy adott egyén az Egyesült Államokon kívül található nem amerikai személy, valamint hogy az e személyre irányuló megfigyelés alkalmas külföldi hírszerzési információk megszerzésére. Az adattakarékossági eljárások a FISA 702. cikke alapján amerikai személlyel kapcsolatosan megszerzett valamennyi, nem nyilvános információ megszerzésére, tárolására, felhasználására és terjesztésére vonatkoznak.

59. A PRISM program keretében az elektronikus hírközlési szolgáltatók kötelesek átadni az NSA részére minden, az utóbbi által közölt kiválasztási tényezőtől „származó” vagy „neki címzett” közlést. E közlések egy részét továbbítják az FBI és a Central Intelligence Agency (CIA) (Központi Hírszerző Ügynökség, Egyesült Államok) felé. 2015-ben 94 386 személyt figyeltek meg, 2011-ben pedig az Egyesült Államok kormánya több mint 250 millió közlést szerzett meg e program keretében.

60. Az Upstream program alapja azon vállalkozások kötelező segítségnyújtása, amelyek a „gerinchálózatot” – vagyis azon kábelek, kapcsolók és routerek hálózatát – üzemeltetik, amelyen továbbítják a telefonos és az internetes közléseket. E vállalkozások kötelesek lehetővé tenni az NSA számára, hogy lemásolják és szűrjék az internetes adatáramlást, annak érdekében, hogy megszerezzék az ügynökség utasításában megjelölt kiválasztási tényezőtől „származó”, „neki címzett” vagy „rá vonatkozó” közlést. A kiválasztási tényezőre „vonatkozó” közlések azokat jelölik, amelyek utalnak e kiválasztási tényezőre, anélkül hogy az említett kiválasztási tényezőhöz kapcsolódó nem amerikai személy abban szükségképpen részt venne. Bár a FISC 2017. április 26-i véleményéből az következik, hogy ezen időponttól kezdődően az amerikai kormány nem gyűjti és nem szerzi meg a kiválasztási tényezőre „vonatkozó” közléseket, e vélemény nem tartalmazza azt, hogy az NSA felhagyott volna a megfigyelő eszközén továbbított kommunikációáramlás lemásolásával és szűrésével. Az Upstream program ily módon azt vonja maga után, hogy az NSA hozzáfér a közlések metaadataihoz és tartalmához is. 2011 óta az NSA évente körülbelül 26,5 millió közlést gyűjtött be az Upstream program keretében, ami ugyanakkor az e program alapján végzett szűrési eljárásnak alávetett közléseknek csak egy kis részét teszi ki.

61. Egyébként a High Court (felsőbíróság) megállapításai szerint az EO 12333 megengedi az elektronikus kommunikáció megfigyelését az Egyesült Államok területén kívül, lehetővé téve külföldi hírszerzési célból a hozzáférést az e terület felé „továbbítás alatt álló”, illetve az e területen „áthaladó”, de nem ottani kezelésre szánt adatokhoz, valamint ezek gyűjtését és tárolását. Az EO 12333 a „külföldi hírszerzés” fogalmát úgy határozza meg, hogy az a külföldi kormányok, külföldi szervezetek, illetve külföldi személyek képességeivel, szándékaival, illetve tevékenységeivel kapcsolatos információkra terjed ki. [17]

62. Az EO 12333 felhatalmazza az NSA-t arra, hogy hozzáférjen az Atlanti-óceán fenekén található tenger alatti kábelekhez, amelyek révén az adatokat az Unióból az Egyesült Államokba továbbítják, azt megelőzően, hogy ezen adatok az Egyesült Államokba érkeznének, és ezáltal a FISA rendelkezéseinek hatálya alá kerülnének. Ugyanakkor nincs bizonyíték semmilyen, ezen elnöki rendelet alapján végrehajtott programot illetően.

63. Noha az EO 12333 rögzít korlátozásokat az információk gyűjtését, tárolását és terjesztését illetően, e korlátozások nem vonatkoznak a nem amerikai személyekre. Az utóbbiakra kizárólag a Presidential Policy Directive 28-ban (28. sz. elnöki politikai irányelv, a továbbiakban: PPD 28) rögzített garanciák vonatkoznak, amely minden jelfelderítési külföldi hírszerzési információ gyűjtésével és felhasználásával kapcsolatos tevékenységre alkalmazandó. A PPD 28 kimondja, hogy a magánélet tiszteletben tartása szerves részét képezi az e tevékenységek tervezése során figyelembe veendő megfontolásoknak, hogy az adatgyűjtés egyetlen célja a külföldi hírszerzési információk megszerzése, illetve a kémelhárítás lehet, továbbá hogy az említett tevékenységeknek „a lehető legcélzottabbaknak kell lenniük”.

64. A kérdést előterjesztő bíróság szerint az NSA EO 12333-on – amelyet az Egyesült Államok elnöke bármikor módosíthat vagy visszavonhat – alapuló tevékenységeit nem törvény szabályozza, azok nem tartoznak bírósági felügyelet alá és nem lehet velük kapcsolatban bírósági jogorvoslattal élni.

17 EO 12333, 3.5. pont e) alpontja.

65. E megállapítások alapján e bíróság úgy véli, hogy az Egyesült Államok tömegesen és megkülönböztetés nélkül kezel személyes adatokat, ami kiteszi az érintetteket azon veszélynek, hogy megsértik az őket a Charta 7. és 8. cikke alapján megillető jogokat.

66. Ezenfelül az említett bíróság kiemeli, hogy nem ugyanazon bírósági jogorvoslatok állnak az uniós polgárok rendelkezésére személyes adataiknak az amerikai hatóságok általi jogellenes kezelése esetében, mint az amerikai állampolgároknak. Az Egyesült Államok Alkotmányának negyedik kiegészítése, amely a legfontosabb védelmet jelenti a jogellenes megfigyeléssel szemben, nem alkalmazható azon uniós polgárokra, akiknek nincs jelentős önkéntes kapcsolatuk az Egyesült Államokkal. Noha az utóbbiakat megilletik bizonyos egyéb jogorvoslatok, azok jelentős akadályokba ütköznek.

67. Közelebbről az Egyesült Államok Alkotmánya alapján a szövetségi bíróságok előtti minden jogorvoslat feltétele az, hogy az érintett bizonyítsa kereshetőségi jogát *(standing)*. A kereshetőségi jog feltétele többek között az, hogy e személy bizonyítsa, hogy valós kárt szenvedett el, amely egyrészt konkrét és részletezett, másrészt bekövetkezett vagy várható. Többek között a Supreme Court of the United States (az Egyesült Államok Legfelsőbb Bírósága) Clapper kontra Amnesty International US ítéletére [18] hivatkozva a kérdést előterjesztő bíróság úgy véli, hogy e feltétel a gyakorlatban rendkívül nehezen teljesíthető, tekintettel többek között arra, hogy semmilyen tájékoztatási kötelezettség nem áll fenn az érintettek felé a velük szemben alkalmazott megfigyelési intézkedések kapcsán. [19] Az uniós polgárok rendelkezésére álló jogorvoslatok egy része esetében ezenkívül további korlátozó feltételek is érvényesülnek, mint a vagyoni kár bizonyításának szükségessége. A hírszerző ügynökségek vonatkozásában elismert szuverén mentesség, valamint az érintett információk titkosítása szintén akadályát képezi egyes jogorvoslati lehetőségek érvényesítésének. [20]

68. A High Court (felsőbíróság) ezenfelül megjelöli a hírszerző ügynökségek tevékenységének különböző felülvizsgálati és felügyeleti mechanizmusait.

69. Ezek közé tartozik egyrészt az, hogy a FISC évente jóváhagyja a FISA 702. cikkén alapuló programokat, ennek során azonban a FISC nem engedélyezi az egyedi kiválasztási tényezőket. Egyebekben semmilyen előzetes bírói felülvizsgálat nem szabályozza a külföldi hírszerzési információk EO 12333 alapján történő gyűjtését.

70. Másrészt a kérdést előterjesztő bíróság utal a hírszerzési tevékenység több bíróságon kívüli felügyeleti mechanizmusára. Hivatkozik különösen az Inspectors General (főellenőrök, Egyesült Államok) szerepére, akiknek feladata az egyes hírszerző ügynökségeken belül a megfigyelési tevékenységek felügyelete. Ezenkívül a Privacy and Civil Liberties Oversight Board (PCLOB) (adatvédelmi és polgári szabadságjog felügyeleti tanács, Egyesült Államok), a végrehajtó hatalmon belül működő független ügynökség jelentéseket kap az egyes ügynökségeken belül polgári szabadságjogi és adatvédelmi tisztviselőként *(civil liberties or privacy officers)* kijelölt személyektől. A PCLOB rendszeresen jelentéseket nyújt be a parlamenti bizottságok és az elnök számára. Az érintett ügynökségeknek a külföldi hírszerzési információk gyűjtésére vonatkozó szabályok és eljárások megsértésével járó eseményekről tájékoztatniuk kell többek között a DNI-t. Ezeket az eseményeket a FISC felé is jelentik. Az Egyesült Államok Kongresszusának, a Képviselőház és a Szenátus hírszerzési bizottsága révén szintén a felelősségi körébe tartozik a külföldi hírszerzési tevékenység felügyelete.

18 133 S.Ct. 1138 (2013).

19 A kérdést előterjesztő bíróság ugyanakkor megállapította, hogy azon elv alól, amely szerint nem kell értesíteni a megfigyelési intézkedéssel érintett személyt, van egy kivétel, amennyiben az amerikai kormány a FISA 702. cikke alapján gyűjtött adatokat fel kívánja használni az említett személlyel szembeni büntető- vagy közigazgatási eljárás során.

20 A kérdést előterjesztő bíróság így rámutatott arra, hogy bár a Judicial Redress Act (JRA) (a bírói jogvédelemről szóló törvény) kiterjesztette a Privacy Act (a magánélet védelméről szóló törvény) rendelkezéseinek hatályát az uniós polgárokra, amely törvény lehetővé teszi a természetes személyek számára, hogy hozzáférjenek az egyes ügynökségek által bizonyos harmadik országokkal kapcsolatban rögzített, rájuk vonatkozó adatokhoz, az NSA nem szerepel a JRA alapján kijelölt ügynökségek között.

71. A High Court (felsőbíróság) ugyanakkor kiemeli az alapvető különbséget egyrészt az adatok jogszerű megszerzésének, illetve a megszerzést követően azok visszaélésszerű használata elkerülésének biztosítását célzó szabályok, másrészt pedig az e szabályok megsértése esetén rendelkezésre álló jogorvoslatok között. Az érintett személyek alapvető jogainak védelme csak akkor biztosított, ha a hatékony jogorvoslati lehetőségek lehetővé teszik számuk jogaik érvényesítését az említett szabályok megsértése esetén.

72. E körülmények között a kérdést előterjesztő bíróság megalapozottnak tartja a DPC által hivatkozott azon érveket, amelyek szerint az amerikai jog által azon személyek jogorvoslati joga kapcsán előírt korlátozások, akiknek adatait az Unióból továbbítják, nem tartják tiszteletben a Charta 47. cikkében biztosított jog lényeges tartalmát és mindenféleképpen aránytalan beavatkozásokat jelentenek e jog gyakorlásába.

73. A High Court (felsőbíróság) szerint az, hogy az Egyesült Államok kormánya bevezette az adatvédelmi pajzsról szóló határozatban ismertetett közvetítési mechanizmust, nem elegendő ezen értékelés megkérdőjelezéséhez. Miután kiemelte, hogy e mechanizmus elérhető azon uniós polgárok számára, akik észszerű alapon úgy vélik, hogy adataikat az ÁSZF-határozatoknak [21] megfelelően továbbították, e bíróság megjegyezte, hogy az ombudsman nem minősül a Charta 47. cikkében foglalt követelményeknek megfelelő bíróságnak, és különösen nem független a végrehajtó hatalomtól. [22] Az említett bíróság számára az is kétséges, hogy az ombudsman eljárása, akinek határozataival szemben nincs helye bírósági jogorvoslatnak, hatékony jogorvoslatnak minősül-e. Ez az eljárás ugyanis nem teszi lehetővé a kártérítés, illetve a jogellenes cselekmények megszüntetésére kötelezés elérését azon személyek számára, akiknek adatait jogellenesen gyűjtötték, kezelték vagy osztották meg, mivel az ombudsman nem erősíti meg, illetve nem is cáfolja, hogy a felperes elektronikus megfigyelési intézkedés tárgya volt.

74. Miután a fentiek szerint ismertette aggályait az amerikai jog által előírt garanciák és a Charta 7., 8. és 47. cikkéből következő követelmények lényegi azonosságát illetően, a kérdést előterjesztő bíróság ismertette az azzal kapcsolatos kérdéseket, hogy az ÁSZF-határozatokban előírt általános szerződési feltételek – amelyek jellegüknél fogva nem kötelezik az amerikai hatóságokat – mindazonáltal alkalmasak-e az érintettek alapvető jogai védelmének biztosítására. E bíróság ebből azt a következtetést vonta le, hogy osztja a DPC e határozatok érvényességével kapcsolatos kétségeit.

75. E tekintetben a kérdést előterjesztő bíróság közelebbről úgy véli, hogy a 95/46 irányelv – 2010/87 határozat 4. cikkében hivatkozott – 28. cikkének (3) bekezdése, amennyiben elismeri a felügyeleti hatóságok hatáskörét az e határozatban előírt általános szerződési feltételeken alapuló adattovábbítás felfüggesztésére vagy megtiltására, nem elegendő e kétségek eloszlatására. Azonkívül, hogy e hatáskör álláspontja szerint pusztán diszkrecionális jellegű, a kérdést előterjesztő bíróság felveti a kérdést, hogy a 2010/87 határozat (11) preambulumbekezdésének fényében van-e lehetőség annak gyakorlására abban az esetben, ha a megállapított hiányosságok nem egyedi és kivételes esetre vonatkoznak, hanem általános és rendszerszerű jellegűek. [23] Úgy véli továbbá, hogy annak veszélye, hogy a különböző tagállamokban eltérő határozatokat hoznak, az ellen szólhatnak, hogy e hiányosságok megállapítását a felügyeleti hatóságokra bízzák.

21 A kérdést előterjesztő bíróság ezzel kapcsolatban az adatvédelmi pajzsról szóló határozat III. A. mellékletére hivatkozik (lásd a jelen indítvány 37. és 38. pontját).

22 A kérdést előterjesztő bíróság a 2005. január 27-i Denuit és Cordenier ítéletre (C-125/04, EU:C:2005:69, 12. pont) hivatkozik.

23 A 2010/87 határozat (11) preambulumbekezdése szerint: „A tagállamok felügyeleti hatóságai kulcsfontosságú szerepet játszanak e szerződéses mechanizmusban, mivel ők biztosítják, hogy a személyes adatok továbbításukat követően megfelelő védelemben részesüljenek. Kivételes esetekben, amikor az adatátadók nem hajlandók vagy nem képesek megfelelő módon tájékoztatni az adatátvevőket – ami az érintettek számára súlyos károkat okozhat –, az általános szerződési feltételeknek lehetővé kell tenniük, hogy a felügyeleti hatóságok ellenőrizhessék az adatátvevőket és további feldolgozókat, és – adott esetben – rájuk nézve kötelező határozatokat hozzanak. A felügyeleti hatóságoknak megfelelő hatáskörrel kell rendelkezniük ahhoz, hogy az általános szerződési feltételek alapján megtiltsanak vagy felfüggesszenek adattovábbítást vagy adattovábbításokat azokban a kivételes esetekben, amikor megállapítást nyer, hogy egy szerződés alapján teljesített adattovábbításnak vélhetően súlyosan hátrányos hatása lesz az érintettek számára megfelelő védelmet biztosító garanciákra és kötelezettségekre.”

76. E körülmények között a High Court (felsőbíróság, Írország) a Bírósághoz 2018. május 9-én érkezett, 2018. május 4-i határozatával[24] az eljárást felfüggesztette, és előzetes döntéshozatal céljából az alábbi kérdéseket terjesztette a Bíróság elé:

„1) Olyan körülmények között, amikor valamely magánvállalkozás az [Unió] tagállamából harmadik országbeli magánvállalkozás részére kereskedelmi célból személyes adatot továbbít [a 2010/87 határozat] alapján, és a szóban forgó harmadik országban annak hatóságai nemzetbiztonsági célból, ezen felül azonban bűnüldözési célból, valamint e harmadik ország külügyi tevékenysége céljából is e személyes adatok további kezelését végezhetik, az EUSZ 4. cikk (2) bekezdésének nemzeti biztonsággal kapcsolatos rendelkezései és a [95/46 irányelv] 3. cikke (2) bekezdésének első francia bekezdésében foglalt, a közbiztonsággal, a védelemmel és a nemzetbiztonsággal kapcsolatos rendelkezései ellenére alkalmazható-e az uniós jog (ideértve [a Chartát]) az adattovábbításra?

2) a) Annak meghatározása során, hogy sérti-e valamely magánszemély jogát az [Unióból] [a 2010/87 határozat] alapján harmadik országba irányuló adattovábbítás, ahol ezeket az adatokat nemzetbiztonsági okból további kezelés alá vonhatják, vajon a vonatkozó összehasonlítási alap [a 95/46 irányelv] értelmében:

i. a Charta, az EUSZ, az EUMSZ, [a 95/46 irányelv], [a Rómában 1950. november 4-én aláírt, az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény {kihirdette: 1993. évi XXXI. törvény, a továbbiakban: EJEE}] (vagy az uniós jog valamely más rendelkezése); vagy

ii. egy vagy több tagállam nemzeti jogszabályai?

b) Amennyiben a [ii. alpont] a vonatkozó összehasonlítási alap, be kell-e vonni az összehasonlítási alapba egy vagy több tagállam nemzetbiztonsággal kapcsolatos gyakorlatát?

3) Annak értékelése során, hogy valamely harmadik ország [a 95/46 irányelv] 26. cikke értelmében biztosítja-e az uniós jog által a szóban forgó országba továbbított személyes adatokkal összefüggésben megkövetelt szintű védelmet, a védelem e harmadik országban biztosított szintjét az alábbiak közül melyekre való hivatkozással kell vizsgálni:

a) a harmadik országban a saját nemzeti jogszabályaiból vagy nemzetközi kötelezettségvállalásaiból eredően alkalmazandó szabályokra, és az e szabályokkal való összhang biztosítását szolgáló gyakorlatra, beleértve a harmadik országban érvényesülő szakmai szabályokat és biztonsági intézkedéseket;

vagy

b) az a) pontban hivatkozott szabályokra az adott harmadik országban fennálló közigazgatási, szabályozási és megfelelőségi gyakorlattal és szakpolitikai biztosítékokkal, eljárásokkal, protokollokkal, felügyeleti mechanizmusokkal és bíróságon kívüli jogorvoslatokkal együtt?

4) Tekintettel a High Court (felsőbíróság) által az Egyesült Államok jogával kapcsolatban tett ténymegállapításokra, sérti-e a magánszemélyeknek a Charta 7. és/vagy 8. cikkében foglalt jogait, ha a személyes adatokat [az Unióból] az Egyesült Államokba [a 2010/87 határozat] alapján továbbítják?

24 A Facebook Ireland az előzetes döntéshozatalra utaló határozattal szemben fellebbezést nyújtott be a Supreme Courthoz (legfelsőbb bíróság, Írország). E fellebbezést a 2019. május 31-i, a The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, Appeal nº 2018/68 ítélet (a továbbiakban: a Supreme Court [legfelsőbb bíróság] 2019. május 31-i ítélete) elutasította.

5) Tekintettel a High Court (felsőbíróság) által az Egyesült Államok jogával kapcsolatban tett ténymegállapításokra, ha a személyes adatokat [az Unióból] az Egyesült Államokba [a 2010/87 határozat] alapján továbbítják:

   a) Az Egyesült Államok által biztosított védelem szintje tiszteletben tartja-e a Charta 47. cikke által a magánszemélyeknek az adatvédelmi jogai megsértése miatti bírósági jogorvoslathoz való joga lényegét?

Az a) kérdésre adott igenlő válasz esetében:

   b) Az Egyesült Államok jogában előírt, valamely magánszemély bírósági jogorvoslathoz való jogának az Egyesült Államok nemzetbiztonságával összefüggésben való korlátozása arányos-e a Charta 52. cikkének értelmében, és nem haladja-e meg azt, ami egy demokratikus társadalomban nemzetbiztonsági szempontból szükséges?

6) a) Milyen szintű védelmet kell biztosítani a harmadik országokba [a 95/46 irányelv 26. cikkének (4) bekezdése] szerint hozott bizottsági határozatnak megfelelően elfogadott általános szerződési feltételek alapján továbbított személyes adatok tekintetében, figyelemmel [ezen] irányelv rendelkezéseire, és különösen a Chartával összhangban értelmezett 25. és 26. cikkére?

   b) Milyen szempontokat szükséges figyelembe venni annak értékelése során, hogy valamely harmadik országba [a 2010/87 határozat] alapján továbbított adatok tekintetében biztosított védelem szintje megfelel-e [a 95/46 irányelvben] és a Chartában foglalt követelményeknek?

7) Az a körülmény, hogy az általános szerződési feltételek az adatátadó és az adatátvevő között érvényesülnek, és valamely harmadik ország nemzeti hatóságaira nézve nem kötelezőek, amely ország előírhatja az adatátadó részére, hogy a biztonsági szolgálatai számára további adatkezelés céljából tegye hozzáférhetővé [a 2010/87 határozatban] megállapított feltételek alapján továbbított személyes adatokat, megakadályozza-e, hogy e feltételek megfelelő garanciákat teremtsenek, amint azt [a 95/46 irányelv] 26. cikkének (2) bekezdése előírja?

8) Amennyiben valamely harmadik országbeli adatátvevő [olyan] felügyeleti jogszabályok hatálya alá tartozik, [amelyek a felügyeleti hatóság] álláspontja szerint [a 2010/87 határozat] mellékletében foglalt feltételekbe, vagy [a 95/46 irányelv] 25. és 26. cikkébe, és/vagy a Charta rendelkezéseibe ütközik, [a felügyeleti hatóság] köteles-e gyakorolni [a 95/46 irányelv] 28. cikkének (3) bekezdése szerinti végrehajtási jogkörét az adatáramlás felfüggesztése iránt vagy az ilyen jogosultságok gyakorlása, figyelemmel [a 2010/87 határozat (11) preambulumbekezdésében] foglaltakra, kizárólag kivételes esetekre korlátozódik, vagy pedig az adatvédelmi hatóság saját mérlegelési jogkörében eljárva dönthet úgy, hogy nem függeszti fel az adatáramlást?

9) a) [A 95/46 irányelv] 25. cikkének (6) bekezdése értelmében [az adatvédelmi pajzsról szóló határozat] olyan általános hatályú, a tagállamok [felügyeleti hatóságaira] és bíróságaira nézve kötelező megállapításnak minősül, amely alapján az [Egyesült Államok] [a 95/46 irányelv] 25. cikkének (2) bekezdése értelmében a nemzeti joga, illetve az általa vállalt nemzetközi kötelezettségek révén megfelelő szintű védelmet biztosít?

   b) Amennyiben nem biztosít megfelelő szintű védelmet, adott esetben milyen jelentősége van [az adatvédelmi pajzsról szóló határozatnak] az Egyesült Államokba [a 2010/87 határozat] alapján továbbított adatok tekintetében nyújtott biztosítékok megfelelőségének vizsgálata során?

10) Tekintettel a High Court (felsőbíróság) által az Egyesült Államok jogával kapcsolatban tett ténymegállapításokra, [az adatvédelmi pajzsról szóló határozat] III. mellékletének A. mellékletében foglalt, adatvédelmi ombudsmanra vonatkozó rendelkezés, amennyiben azt az Egyesült Államok fennálló rendszerével összefüggésben értelmezzük, gondoskodik-e arról, hogy az

Egyesült Államok a Charta 47. cikkével összeegyeztethető jogorvoslatot biztosít azon érintettek számára, akiknek a személyes adatait [a 2010/87 határozat] alapján az Egyesült Államokba továbbítják?

11) Sérti-e [a 2010/87 határozat] a Charta 7., 8. és/vagy 47. cikkében foglaltakat?"

77. A DPC, a Facebook Ireland, M. Schrems, az Egyesült Államok kormánya, az EPIC, a BSA, a Digitaleurope, Írország, a belga, a cseh, a német, a holland, az osztrák, a lengyel, a portugál kormány, az Egyesült Királyság kormánya, az Európai Parlament, valamint a Bizottság terjesztett elő írásbeli észrevételeket a Bíróság előtt. A DPC, a Facebook Ireland, M. Schrems, az Egyesült Államok kormánya, az EPIC, a BSA, a Digitaleurope, Írország, a német, a francia, a holland, az osztrák kormány, az Egyesült Királyság kormánya, a Parlament, a Bizottság, valamint az Európai Adatvédelmi Testület (European Data Protection Board, EDPB) képviseltette magát a 2019. július 9-i tárgyaláson.

IV. Elemzés

A. Előzetes megfontolások

78. Azt követően, hogy a Bíróság a Schrems ítéletben érvénytelenné nyilvánította a „biztonságos kikötő" határozatot, a személyes adatok Egyesült Államokba történő továbbítása más jogalapokon folytatódott. Közelebbről, az adatátadó társaságok olyan szerződéseket köthettek az adatátvevőkkel, amelyek tartalmazzák a Bizottság által kidolgozott általános szerződési feltételeket. E feltételek képezik a jogalapját a számos olyan más országba irányuló adattovábbításoknak, amelyek kapcsán a Bizottság nem hozott megfelelőségi szóló határozatot.[25] Az adatvédelmi pajzsról szóló határozat immár lehetővé teszi az említett határozatban rögzített elvekhez csatlakozásról öntanúsítással rendelkező vállalkozások számára a személyes adatok további alaki követelmények nélküli továbbítását az Egyesült Államokba.

79. Amint azt az előzetes döntéshozatalra utaló határozat kifejezetten kiemeli és amint azt a BSA, a Digitaleurope, Írország, az osztrák és a francia kormány, a Parlament, valamint a Bizottság hangsúlyozza, a High Court (felsőbíróság) előtt folyamatban lévő alapeljárás egyetlen tárgya annak eldöntése, hogy érvényes-e az a határozat, vagyis a 2010/87 határozat, amely révén a Bizottság bevezette az M. Schrems panaszában említett adattovábbítások alátámasztása céljából hivatkozott általános szerződési feltételeket.[26]

80. A jogvita alapja egy panasz, amelyben a DPC azt kérte a kérdést előterjesztő bíróságtól, hogy előzetes döntéshozatal céljából terjesszen a 2010/87 határozat érvényességére vonatkozó kérdést a Bíróság elé. E bíróság szerint az alapeljárás ily módon azon jogorvoslat gyakorlását érinti, amelynek tagállamok általi bevezetését a Bíróság a Schrems ítélet 65. pontjában írta elő.

81. Emlékeztetőül, ezen ítélet 63. pontjában a Bíróság azt mondta ki, hogy a felügyeleti hatóság köteles a kellő gondossággal megvizsgálni az olyan panaszt, amelynek keretében egy olyan személy, akinek a személyes adatait olyan harmadik országba továbbították vagy továbbíthatják, amely megfelelőségi határozat tárgyát képezi, vitatja e határozat összeegyeztethetőségét a Chartában rögzített alapvető jogokkal. Az említett ítélet 65. pontja szerint, amennyiben az említett hatóság megalapozottnak ítéli meg az e panaszban felhozott kifogásokat, a 95/46 irányelvnek – a Charta 8. cikke (3) bekezdésével

25 A BSA állítása szerint az e szövetséghez tartozó, az ezzel kapcsolatos vizsgálat során választ adó vállalkozások 70%-a jelezte, hogy a személyes adatok harmadik országokba való továbbításának elsődleges jogalapjaként általános szerződési feltételekre támaszkodik. A Digitaleurope is úgy véli, hogy az általános szerződési feltételek jelentik az ilyen adattovábbítások alátámasztása céljából hivatkozott elsődleges jogi eszközt.

26 Noha a kérdést előterjesztő bíróság kiemeli, hogy előzetes döntéshozatal iránti kérelme mindhárom ÁSZF-határozat érvényességére vonatkozik, mivel azokat a DPC határozattervezetében, valamint a 2017. október 3-i ítéletben vizsgálták meg, az előzetes döntéshozatalra előterjesztett kérdések kizárólag a 2010/87 határozatra vonatkoznak. Ugyanez a helyzet amiatt is, hogy e bíróság előtt a Facebook Ireland e határozatot jelölte meg a Facebook közösségi háló európai felhasználói személyes adatai Egyesült Államokba történő továbbításának jogalapjaként. Elemzésem tehát kizárólag e határozatra vonatkozik.

összefüggésben értelmezett – 28. cikke (3) bekezdése harmadik albekezdésének harmadik francia bekezdése alapján (amelynek a GDPR 58. cikkének (5) bekezdése felel meg) lehetőséggel kell rendelkeznie arra, hogy bírósági eljárást indítson. E tekintetben a nemzeti jogalkotónak olyan jogorvoslati lehetőségeket kell kialakítania, amelyek lehetővé teszik e hatóság számára, hogy a nemzeti bíróságok előtt e kifogásokra hivatkozzon annak érdekében, hogy amennyiben az utóbbiak osztják e hatóság kétségeit, előzetes döntéshozatali eljárást kezdeményezhessenek e határozat érvényessége kapcsán.

82. A kérdést előterjesztő bírósághoz hasonlóan úgy vélem, hogy e következtetések analógia útján alkalmazandók, amennyiben a felügyeleti hatóságnak az elé terjesztett panasz elbírálása során nem egy megfelelőségi határozat, hanem egy a 2010/87 határozathoz hasonló, a személyes adatok harmadik országba való továbbítása céljából általános szerződési feltételeket megállapító határozat érvényessége kapcsán vannak kétségei. Ellentétben a német kormány által előadottakkal, nem releváns, hogy e kétségek a panaszos által e hatóság tudomására hozott kifogásoknak felelnek-e meg, vagy pedig e hatóság saját kezdeményezésére kérdőjelezi meg a szóban forgó határozat érvényességét. A Bíróság indokolásának alapját képező, a GDPR 58. cikkének (5) bekezdéséből és a Charta 8. cikkének (3) bekezdéséből következő követelmények ugyanis attól függetlenül alkalmazandók, hogy mi a felügyeleti hatóságokhoz benyújtott panaszban hivatkozott adattovábbítás jogalapja és milyen indokok alapozták meg a panasz elbírálása során e hatóság kétségét az érintett határozat érvényességét illetően.

83. Ezt leszögezve, a DPC azzal az indokkal kérte a kérdést előterjesztő bíróságtól, hogy intézzen kérdést a Bírósághoz a 2010/87 határozat érvényességét illetően, hogy álláspontja szerint szükséges a Bíróság felvilágosítása azon panasz elbírálásához, amely révén M. Schrems azt kéri tőle, hogy a 95/46 irányelv 28. cikke (3) bekezdésének második francia bekezdésében ráruházott – azóta pedig a GDPR 58. cikke (2) bekezdésének f) pontjában részére biztosított – hatáskört gyakorolva függessze fel M. Schrems személyes adatainak Facebook Ireland általi továbbítását a Facebook Inc. részére.

84. Ily módon, míg az alapeljárás kizárólag a 2010/87 határozat *in abstracto* érvényességére vonatkozik, addig a DPC előtt folyamatban levő mögöttes eljárás tárgya a DPC részéről arra irányuló hatáskörének gyakorlása, hogy *egy konkrét ügyben* korrekciós intézkedéseket fogadjon el. Azt javaslom a Bíróságnak, hogy a 2010/87 határozat érvényességének meghatározásához szükséges mértékben szorítkozzon az előterjesztett kérdések vizsgálatára, mivel e vizsgálat elegendő a kérdést előterjesztő bíróság számára az előtte folyamatban levő eljárás elbírálásához.[27]

85. E határozat érvényességének értékelését megelőzően el kell utasítani az előzetes döntéshozatal iránti kérelem elfogadhatóságával kapcsolatban felhozott kifogást.

B. Az előzetes döntéshozatal iránti kérelem elfogadhatóságáról

86. Az előzetes döntéshozatal iránti kérelem elfogadhatóságát különböző okok miatt vitatták, amelyek lényegében az előzetes döntéshozatalra előterjesztett kérdésekben hivatkozott 95/46 irányelv *ratione temporis* alkalmazhatatlanságára (1. rész), illetve arra vonatkoztak, hogy a DPC előtt folyó eljárás nem jutott kellően előrehaladott szakaszba ahhoz, hogy igazolja a kérelem szükségességét (2. rész), továbbá arra, hogy bizonytalanságok maradtak fenn a kérdést előterjesztő bíróság által ismertetett ténybeli hátteret illetően (3. rész).

27 Lásd a jelen indítvány 167–186. pontját.

87. Ezen elfogadhatatlansági kifogásokra az EUMSZ 267. cikk alapján a Bíróság elé terjesztett kérdések relevanciájának vélelmét szem előtt tartva fogok válaszolni. Az állandó ítélkezési gyakorlat szerint a Bíróság csak akkor utasíthatja el az előzetes döntéshozatal iránti kérelmet, ha az uniós jog kért értelmezése nyilvánvalóan semmilyen összefüggésben nincs az alapügy tényállásával vagy tárgyával, ha a probléma hipotetikus jellegű, vagy ha nem állnak a Bíróság rendelkezésére azok a ténybeli vagy jogi elemek, amelyek szükségesek ahhoz, hogy az elé terjesztett kérdésekre hasznos választ adhasson.[28]

1. A 95/46 irányelv időbeli hatályáról

88. A Facebook Ireland az előzetes döntéshozatalra előterjesztett kérdések elfogadhatatlanságára hivatkozik, azzal az indokkal, hogy azok a 95/46 irányelvre hivatkoznak, holott ezt az irányelvet a GDPR 2018. május 25-i hatállyal hatályon kívül helyezte és felváltotta.[29]

89. Egyetértek azzal az álláspontttal, amely szerint a 2010/87 határozat érvényességét a GDPR rendelkezéseinek fényében kell megvizsgálni.

90. E rendelet 94. cikkének (2) bekezdése szerint „[a] hatályon kívül helyezett irányelvre történő hivatkozásokat az [említett] rendeletre történő hivatkozásnak kell tekinteni”. Ebből álláspontom szerint az következik, hogy a 2010/87 határozatot, amennyiben jogalapként a 95/46 irányelv 26. cikkének (4) bekezdésére hivatkozik, úgy kell értelmezni, mint amely az említett rendelkezés tartalmát lényegében átvevő GDPR 46. cikke (2) bekezdésének c) pontjára hivatkozik.[30] Következésképpen a Bizottság által a 95/46 irányelv 26. cikkének (4) bekezdése alapján a GDPR hatálybalépése előtt elfogadott végrehajtási határozatokat e rendeletre figyelemmel kell értelmezni. Szintén e rendelet alapján kell adott esetben értékelni azok érvényességét.

91. E következtetést nem kérdőjelezi meg az az ítélkezési gyakorlat, amely szerint az uniós intézkedések jogszerűségét az intézkedés meghozatalának időpontjában fennálló ténybeli és jogi elemek függvényében kell elbírálni. Ez az ítélkezési gyakorlat ugyanis a jogi aktus érvényességének a meghozatala időpontjában releváns ténybeli körülményekre,[31] illetve a meghozatalát szabályozó eljárási szabályokra[32] figyelemmel történő vizsgálatára vonatkozik. Ezzel szemben a Bíróság a másodlagos jogi aktusok érvényességét visszatérően az e jogi aktusok meghozatalát követően hatályba lépett magasabb szintű normákra figyelemmel vizsgálta.[33]

92. Ugyanakkor az előzetes döntéshozatalra előterjesztett kérdések szövegében egy olyan jogi aktus megjelölése, amely *ratione temporis* már nem alkalmazható, noha a kérdések átfogalmazását indokolttá teszi, nem vonhatja maga után az elfogadhatatlanságot.[34] Amint azt a DPC és M. Schrems kifejtik, az előzetes döntéshozatalra előterjesztett kérdések szövegében a 95/46 irányelvre való hivatkozásokat egyébként a jelen üggyel kapcsolatos eljárás ütemezése is igazolhatja, mivel e kérdéseket a GDPR hatálybalépése előtt terjesztették a Bíróság elé.

28 Lásd többek között: 2018. december 10-i Wightman és társai ítélet (C-621/18, EU:C:2018:999, 27. pont); 2019. november 19-i A. K. és társai ítélet (A legfelsőbb bíróság fegyelmi tanácsának függetlensége) (C-585/18, C-624/18 és C-625/18, EU:C:2019:982, 98. pont).

29 Lásd a GDPR 94. cikkének (1) bekezdését és 99. cikkének (1) bekezdését.

30 Hangsúlyozom, hogy a GDPR 46. cikke (5) bekezdésének megfelelően a Bizottság által a 95/46 irányelv 26. cikkének (4) bekezdése alapján elfogadott határozatok mindaddig hatályban maradnak, amíg nem módosítják, nem váltják fel vagy nem helyezik hatályon kívül azokat.

31 Lásd többek között: 1979. február 7-i Franciaország kontra Bizottság ítélet (15/76 és 16/76, EU:C:1979:29, 7. pont); 2001. május 17-i IECC kontra Bizottság ítélet (C-449/98 P, EU:C:2001:275, 87. pont); 2013. október 17-i Schaible ítélet (C-101/12, EU:C:2013:661, 50. pont).

32 Lásd többek között: 2015. április 16-i Parlament kontra Tanács ítélet (C-540/13, EU:C:2015:224, 35. pont); 2015. április 16-i Parlament kontra Tanács ítélet (C-317/13 és C-679/13, EU:C:2015:223, 45. pont); 2016. szeptember 22-i Parlament kontra Tanács ítélet (C-14/15 és C-116/15, EU:C:2016:715, 48. pont).

33 Közelebbről a Schrems ítéletben a Bíróság a „biztonságos kikötő” határozat érvényességét a Charta rendelkezéseire figyelemmel értékelte, amelynek elfogadására e határozat meghozatalát követően került sor. Lásd még: 2011. március 17-i AJD Tuna ítélet (C-221/09, EU:C:2011:153, 48. pont); 2015. június 11-i Pfeifer & Langen ítélet (C-51/14, EU:C:2015:380, 42. pont).

34 Lásd többek között: 2010. július 15-i Pannon Gép Centrum ítélet (C-368/09, EU:C:2010:441, 30–35. pont); 2011. február 10-i Andersson ítélet (C-30/10, EU:C:2011:66, 20. és 21. pont); 2018. október 25-i Roche Lietuva ítélet (C-413/17, EU:C:2018:865, 17–20. pont).

93. Mindenesetre a GDPR azon rendelkezései, amelyeket az előzetes döntéshozatalra előterjesztett kérdések elemzése céljából tárgyalok – vagyis különösen a 45., 46. és 58. cikk – lényegében átveszik a 95/46 irányelv 25., 26. és 28. cikkének tartalmát, ugyanakkor fejlesztve és némiképp árnyalva azt. Ami ezek a 2010/87 határozat érvényességének elbírálása szempontjából való relevanciáját illeti, nem látom okát annak, hogy a GDPR e rendelkezéseinek a 95/46 irányelv megfelelő rendelkezéseitől eltérő tartalmat tulajdonítsak. [35]

2. A DPC által ismertetett kétségek ideiglenes jellegéről

94. A német kormány szerint az előzetes döntéshozatal iránti kérelem elfogadhatatlan, mivel a Schrems ítélet 65. pontjában hivatkozott jogorvoslati eljárás azt feltételezi, hogy a felügyeleti hatóság végleges véleményt alakított ki a felperes által a szóban forgó határozat érvényességével szemben kifejtett kifogások megalapozottságát illetően. Ez álláspontja szerint a jelen ügyben nem áll fenn, mivel a DPC a 2010/87 határozat érvényességével kapcsolatos, egyébként M. Schrems által sem vitatott kétségeit egy ideiglenes határozat tervezetében ismertette, a Facebook Ireland és M. Schrems által esetlegesen benyújtott további észrevételeket nem sértve.

95. Véleményem szerint a DPC által ismertetett kétségek ideiglenes jellege nincs kihatással az előzetes döntéshozatal iránti kérelem elfogadhatóságára. Az előzetes döntéshozatalra előterjesztett kérdés elfogadhatóságának feltételeit ugyanis a jogvita kérdést előterjesztő bíróság által meghatározott tárgyára figyelemmel kell értékelni. [36] Márpedig nem vitatott, hogy az a 2010/87 határozat érvényességére vonatkozik. Az előzetes döntéshozatalra utaló határozat és az ahhoz csatolt ítélet megfogalmazása szerint e bíróság úgy vélte, hogy a DPC által ismertetett kétségek – függetlenül attól, hogy azok ideiglenesek vagy véglegesek – megalapozottak, és ezért kérdést intézett a Bírósághoz az említett határozat érvényességére vonatkozóan. E körülmények között a Bíróság e tárgyban adandó felvilágosítása kétséget kizáróan releváns a kérdést előterjesztő bíróság számára az elé terjesztett jogvita eldöntése céljából.

3. A ténybeli háttér meghatározása körüli bizonytalanságokról

96. Az Egyesült Királyság kormánya szerint a kérdést előterjesztő bíróság által ismertetett ténybeli háttér több olyan hiányosságot tartalmaz, amely elfogadhatatlanná teszi az előzetes döntéshozatalra előterjesztett kérdéseket. E bíróság nem tette egyértelművé, hogy M. Schrems személyes adatait ténylegesen továbbították-e az Egyesült Államokba, illetve igenlő válasz esetén, hogy azokat az amerikai hatóságok gyűjtötték-e. Ezen esetleges adattovábbítások jogalapjának biztos azonosítása is elmaradt, az előzetes döntéshozatalra utaló határozat ugyanis pusztán arra utal, hogy a Facebook közösségi háló európai felhasználóinak adatait „nagyrészt” a 2010/87 határozat által előírt általános szerződési feltételek alapján továbbították. Semmiféleképpen sem bizonyították, hogy a Facebook Ireland és a Facebook Inc. között kötött, a vitatott adattovábbítás alátámasztása céljából hivatkozott szerződés hűen átveszi e feltételeket. A német kormány vitatja továbbá azon indok alapján is az előzetes döntéshozatalra utalás elfogadhatóságát, hogy a kérdést előterjesztő bíróság nem vizsgálta meg, hogy M. Schrems kétséget kizáróan hozzájárult-e a szóban forgó adattovábbításokhoz, amely esetben azok megalapozottan alapultak volna a 95/46 irányelv 26. cikkének (1) bekezdésén (amelynek tartalmát a GDPR 49. cikke (1) bekezdésének d) pontja lényegében átveszi).

97. Ezek az érvek egyáltalán nem kérdőjelezik meg az előzetes döntéshozatalra utalás relevanciáját az alapeljárás tárgya szempontjából. Mivel a jogvita abból ered, hogy a DPC élt a Schrems ítélet 65. pontjában előírt jogorvoslattal, e jogvita arra irányul, hogy a nemzeti bíróság terjesszen elő előzetes döntéshozatal iránti kérelmet a 2010/87 határozat érvényességét illetően. A német kormány, valamint

35 Lásd e tekintetben: Bobek főtanácsnok Fashion ID ügyre vonatkozó indítványa (C-40/17, EU:C:2018:1039, 87. pont).

36 Lásd a jelen indítvány 87. pontját.

az Egyesült Királyság kormánya az előzetes döntéshozatalra előterjesztett kérdések szükségességét valójában nem az említett határozat érvényességének eldöntése céljából vitatja, hanem annak érdekében, hogy lehetővé tegye a DPC számára, hogy konkrét döntést hozzon M. Schrems panaszát illetően.

98. Mindenesetre még ezen, az alapeljárás mögött meghúzódó eljárás szempontjából sem tűnnek irrelevánsnak a 2010/87 határozat érvényességére vonatkozóan előzetes döntéshozatalra előterjesztett kérdések. A kérdést előterjesztő bíróság ugyanis megállapította, hogy a Facebook Ireland a „biztonságos kikötő” határozat érvénytelenné nyilvánítását követően is folytatta felhasználói adatainak továbbítását az Egyesült Államokba, valamint hogy ezen adattovábbítások legalábbis részben a 2010/87 határozaton alapultak. Ezenfelül, noha hasznos lenne, ha az összes releváns tény megállapítására sor kerülne az EUMSZ 267. cikken alapuló hatáskörének gyakorlását megelőzően, kizárólag a kérdést előterjesztő bíróságra tartozik annak értékelése, hogy az eljárás mely szakaszában van szüksége a Bíróság előzetes döntésére.[37]

99. A fentiek összességére figyelemmel úgy vélem, hogy az előzetes döntéshozatal iránti kérelem elfogadható.

C. Az uniós jognak a személyes adatok olyan harmadik országba történő, kereskedelmi célú továbbításaira való alkalmazhatóságáról, ahol azokat nemzetbiztonsági célból használhatják fel (első kérdés)

100. Első kérdésével a kérdést előterjesztő bíróság azt kívánja megtudni, hogy az uniós jog alkalmazandó-e a személyes adatok valamely tagállambeli társaság által harmadik országban székhellyel rendelkező társaság részére kereskedelmi okokból végzett továbbítására, amennyiben az adattovábbítás megkezdését követően az adatokat a harmadik ország hatóságai a nemzetbiztonság védelmére kiterjedő célokból kezelhetik.

101. E kérdés tétje az alapeljárás eldöntése szempontjából abban rejlik, hogy amennyiben az ilyen adattovábbítás kívül esne az uniós jog hatályán, a 2010/87 határozat érvényességével szemben a jelen ügyben felhozott valamennyi kifogás alaptalannak bizonyulna.

102. Amint azt a kérdést előterjesztő bíróság megjegyezte, a nemzetbiztonsági célú adatkezelések a 95/46 irányelv 3. cikkének (2) bekezdése alapján ki voltak zárva az irányelv hatálya alól. A GDPR 2. cikkének (2) bekezdése immár rögzíti, hogy e rendelet nem alkalmazandó többek között a személyes adatok uniós jog hatályán kívül eső tevékenységek során történő kezelésére, illetve a közbiztonság védelme terén illetékes hatóságok által végzett kezelésére. E rendelkezések azt tükrözik, hogy az EUSZ 4. cikk (2) bekezdése elismeri a tagállami hatáskörök fenntartását a nemzetbiztonság területén.

103. A DPC, M. Schrems, Írország, a német, az osztrák, a belga, a cseh, a holland, a lengyel és a portugál kormány, valamint a Parlament és a Bizottság előadja, hogy az M. Schrems panaszában hivatkozottakhoz hasonló adattovábbítások nem tartoznak e rendelkezések hatálya alá, és így az uniós jog alkalmazási körébe esnek. A Facebook Ireland ellentétes álláspontot képvisel. Az előbbiek álláspontjával értek egyet.

37 Lásd ebben az értelemben: 1982. április 1-jei Holdijk és társai ítélet (141/81–143/81, EU:C:1982:122, 5. pont); 2003. december 9-i Gasser ítélet (C-116/02, EU:C:2003:657, 27. pont).

104. E tekintetben fontos kiemelni, hogy a személyes adatok valamely tagállamból egy harmadik országba továbbítása önmagában a valamely tagállam területén végzett, a GDPR 4. cikkének (2) bekezdése értelmében vett „adatkezelésnek” minősül.[38] Az előzetes döntéshozatalra előterjesztett első kérdés tárgya éppen annak eldöntése, hogy alkalmazandó-e az uniós jog azon *adatkezelésre, amelyet maga az adattovábbítás képez*. E kérdés nem arra vonatkozik, hogy alkalmazható-e az uniós jog az Egyesült Államokba továbbított adatok amerikai hatóságok által nemzetbiztonsági céllal végzett esetleges későbbi továbbításaira, amelyek nem tartoznak a GDPR területi hatálya alá.[39]

105. Ebből a szempontból annak eldöntése céljából, hogy az uniós jog alkalmazandó-e a szóban forgó adattovábbításra, kizárólag azon tevékenységet kell figyelembe venni, amelybe az adattovábbítás illeszkedik, a továbbított adatok kapcsán a célországnak számító harmadik ország hatóságai által esetlegesen végzett későbbi adatkezelések céljától függetlenül.[40]

106. Márpedig az előzetes döntéshozatalra utaló határozatból kitűnik, hogy az M. Schrems panaszában hivatkozott adattovábbítás kereskedelmi tevékenység részét képezi. Erre az adattovábbításra egyébként nem a szóban forgó adatok amerikai hatóságok általi későbbi nemzetbiztonsági célú kezelésének lehetővé tétele érdekében került sor.

107. Mindemellett a Facebook Ireland által javasolt megközelítés megfosztaná hatékony érvényesülésétől a GDPR harmadik országba irányuló adattovábbításról szóló rendelkezéseit, mivel soha nem zárható ki, hogy a kereskedelmi tevékenység keretében továbbított adatokat a továbbítást követően nemzetbiztonsági célból kezelik.

108. Az általam javasolt értelmezést támasztja alá a GDPR 45. cikke (2) bekezdése a) pontjának szövege is. E rendelkezés szerint, amikor megfelelőségi határozatot hoz, a Bizottság figyelembe veszi többek között az érintett harmadik ország *nemzetbiztonsági* jogszabályait. Ebből levezethető, hogy annak lehetősége, hogy az adatokat a célországnak számító harmadik ország hatóságai nemzetbiztonsági célból kezelik, nem teszi alkalmazhatatlanná az uniós jogot az adatok e harmadik országba való továbbítása által képzett adatkezelés tekintetében.

109. A Bíróság által a Schrems ítéletben követett okfejtés, illetve az elfogadott következtetések szintén ezen az előfeltevésen alapulnak. A Bíróság így ebben az ítéletben a 95/46 irányelv Charta fényében értelmezett 25. cikkének (6) bekezdése szempontjából vizsgálta meg a „biztonságos kikötő” határozat érvényességét, amennyiben az a személyes adatok Egyesült Államokba való továbbítására vonatkozott, ahol fennállt a lehetősége annak, hogy azokat a nemzetbiztonság védelmét szolgáló célokból gyűjtik és kezelik.[41]

38 Lásd ebben az értelemben: 2006. május 30-i Parlament kontra Tanács és Bizottság ítélet (C-317/04 és C-318/04, EU:C:2006:346, a továbbiakban: PNR-ítélet, 56. pont), valamint Schrems ítélet (45. pont). A GDPR 4. cikkének (2) bekezdése lényegében átveszi az „adatkezelés” 95/46 irányelv 2. cikkének b) pontjában szereplő fogalmát.

39 A GDPR 3. cikkének (1) bekezdése szerint e rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett valamennyi adatkezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik, vagy sem. Az uniós jog Unión kívüli, harmadik ország hírszerző szolgálata által végzett adatkezelésekre való alkalmazhatóságának kérdését meg kell különböztetni az ezen adatkezelésekhez a szóban forgó harmadik országban kapcsolódó szabályok és gyakorlatok által annak eldöntése szempontjából képviselt relevancia kérdésétől, hogy e harmadik országban megfelelő védelmi szintet biztosítanak-e. Az utóbbi témakör képezi az előzetes döntéshozatalra előterjesztett második kérdés tárgyát, és azt a jelen indítvány 201–229. pontjában tárgyalom.

40 A Ministerio Fiscal ügyre vonatkozó indítványomban (C-207/16, EU:C:2018:300, 47. pont) hangsúlyoztam a különbséget egyrészt a személyes adatok államhatalmi tevékenységek során végzett közvetlen kezelése, másrészt pedig a kereskedelmi célú, később hatósági felhasználás által követett adatkezelés között.

41 Ugyanilyen módon a 2017. július 26-i 1/15 (EU-Kanada PNR-megállapodás) véleményében a Bíróság megvizsgálta, hogy összeegyeztethető-e a Charta 7., 8. és 47. cikkével egy olyan, Kanada és az Unió közötti megállapodás tervezete, amely azon adatokra vonatkozik, amelyeket a Kanadába történő továbbítást követően a hatóságok nemzetbiztonsági célból kezelnek.

110. E megfontolásokra figyelemmel úgy vélem, hogy az uniós jog akkor alkalmazandó a személyes adatok valamely tagállamból egy harmadik országba való továbbítására, ha ez az adattovábbítás kereskedelmi tevékenység keretében zajlik, anélkül hogy jelentősége lenne annak, hogy a továbbított adatok esetében fennáll-e annak kockázata, hogy azokat e harmadik országbeli hatóságok a nemzetbiztonság védelme céljából kezelik.

D. Az általános szerződési feltételeken alapuló adattovábbítás során megkövetelt védelmi szintről (a hatodik kérdés első része)

111. Hatodik kérdésének első része szerint az előterjesztő bíróság azt kívánja megtudni, hogy az érintettek alapvető jogai védelmének milyen szintjét kell biztosítani ahhoz, hogy a személyes adatokat a 2010/87 határozatban előírt általános szerződési feltételek alapján továbbítani lehessen harmadik országba.

112. E bíróság hangsúlyozza, hogy a Schrems ítéletben a Bíróság úgy értelmezte a 95/46 irányelv 25. cikkének (6) bekezdését (amelynek tartalmát a GDPR 45. cikkének (3) bekezdése lényegében átvette), amennyiben az azt írja elő, hogy a Bizottság csak azt követően hozhat megfelelőségi határozatot, hogy meggyőződött arról, hogy az érintett harmadik ország *megfelelő* védelmi szintet biztosít, hogy az azt feltételezi, hogy a Bizottság megállapítja, hogy az említett ország ténylegesen az Unióban a Chartával összefüggésben értelmezett 95/46 irányelv által biztosított védelmi szinttel *lényegében azonos* védelmi szintet biztosít az alapvető jogok és szabadságok számára.[42]

113. Ebben az összefüggésben az előzetes döntéshozatalra előterjesztett hatodik kérdés első része annak meghatározására kéri a Bíróságot, hogy a Bizottság által a 95/46 irányelv 25. cikkének (6) bekezdése alapján elfogadott „általános szerződési feltételeknek” – amelyek megfelelnek az azóta a GDPR 46. cikke (2) bekezdésének c) pontjában hivatkozott „általános adatvédelmi kikötéseknek” – ugyanazon, „lényegében azonos” követelménynek megfelelő védelmi szint elérését kell lehetővé tenniük.

114. Ezzel összefüggésben a GDPR 46. cikkének (1) bekezdése azt írja elő, hogy megfelelőségi határozat hiányában az adatkezelő csak abban az esetben továbbíthat személyes adatokat harmadik országba, ha „*megfelelő garanciákat* nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre” (kiemelés tőlem).[43] A GDPR 46. cikke (2) bekezdésének c) pontja szerint e garanciák többek között a Bizottság által kidolgozott általános adatvédelmi kikötésekből következhetnek.

115. A DPC-hez, M. Schrems-hez és Írországhoz hasonlóan úgy vélem, hogy az adatkezelő által nyújtott „megfelelő garanciáknak”, amelyekre a GDPR 46. cikkének (1) bekezdése hivatkozik, azt kell biztosítaniuk, hogy azon személyek jogai, akiknek az adatait továbbítják, ahogy a megfelelőségi határozaton alapuló adattovábbítás esetében is, lényegében azonos védelemben részesüljenek, mint amely a Charta fényében értelmezett GDPR-ből következik.

116. A fenti következtetés e rendelkezés céljából, valamint azon jogi aktusból adódik, amelynek e rendelkezés részét képezi.

42 Schrems ítélet (73. pont). A Bíróság megerősítette e megállapítást az 1/15 véleményben (134. pont).

43 A 95/46 irányelv 26. cikkének (2) bekezdése azt írta elő, hogy a tagállam akkor engedélyezhet ilyen adattovábbítást, „amennyiben az adatkezelő *megfelelő garanciákat* teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelme, továbbá a kapcsolódó jogok gyakorlása tekintetében” (kiemelés tőlem). Az e rendelkezésben hivatkozott „megfelelő garanciák” és a GDPR 46. cikkének (1) bekezdésében hivatkozott „megfelelő garanciák” fogalom tartalma álláspontom szerint megegyezik.

117. A GDPR 45. és 46. cikkének célja a személyes adatok e rendelet által biztosított magas szintű védelmének fenntartása, amennyiben azokat az Unión kívülre továbbítják. A GDPR „Az adattovábbításra vonatkozó általános elv” című 44. cikke ugyanis a harmadik országokba irányuló adattovábbításokkal kapcsolatos V. fejezet legelején szerepel, és kimondja, hogy e fejezet valamennyi rendelkezését úgy kell alkalmazni, hogy a természetes személyek számára a GDPR-ben garantált védelem szintje ne sérüljön harmadik országba történő adattovábbítás esetén.[44] E szabály célja annak elkerülése, hogy az uniós jogból következő védelmi követelményeket ne lehessen megkerülni a személyes adatok harmadik országba való továbbításával, az ottani kezelés céljából.[45] E cél szempontjából közömbös, hogy az adattovábbítás megfelelőségi határozaton, vagy pedig az adatkezelő által többek között szerződési feltételek révén biztosított garanciákon alapul. A Charta által biztosított alapvető jogok védelmi követelményeit illetően nincs különbség azon jogalaptól függően, amelyen az adott adattovábbítás alapul.[46]

118. Ezzel szemben a magas szintű védelem fenntartásának módja eltér az adattovábbítás jogalapjától függően.

119. Egyrészt a megfelelőségi határozat tárgya annak megállapítása, hogy az érintett harmadik ország maga biztosít lényegében azonos védelmet azzal, amelyet az Unión belül kell elérni. A megfelelőségi határozat elfogadásának feltétele, hogy a Bizottság egy adott harmadik ország kapcsán előzetesen értékeli az e harmadik ország joga és gyakorlatai által garantált védelmi szintet, a GDPR 45. cikkének (3) bekezdésében rögzített tényezők fényében. A személyes adatok ilyen esetben anélkül továbbíthatók az említett harmadik országba, hogy az adatkezelőnek külön engedélyt kellene beszereznie.

120. Másrészt, amint azt a következő részben részletesebben kifejtem, az adatkezelő által nyújtott megfelelő garanciák célja magas védelmi szint biztosítása abban az esetben, amikor nem állnak rendelkezésre megfelelő garanciák a célországnak számító harmadik országban. Ily módon, noha a GDPR 46. cikkének (1) bekezdése lehetővé teszi a személyes adatok továbbítását olyan harmadik országba, amely nem biztosít megfelelő szintű védelmet, e rendelkezés csak akkor engedélyezi az ilyen adattovábbításokat, ha más módon nyújtanak megfelelő garanciákat. A Bizottság által elfogadott általános szerződési feltételek e tekintetben az adattovábbításokra a célországnak számító harmadik országtól és az ott biztosított védelmi szinttől függetlenül alkalmazandó általános mechanizmust képeznek.

E. A 2010/87 határozat érvényességéről a Charta 7., 8. és 47. cikke fényében (hetedik, nyolcadik és tizenegyedik kérdés)

121. Hetedik kérdésével az előterjesztő bíróság lényegében azt kívánja megtudni, hogy a 2010/87 határozat érvénytelen-e amiatt, hogy nem kötelező azokra a harmadik országbeli hatóságokra nézve, amelyek felé az e határozat mellékletében előírt általános szerződési feltételek alapján az adatokat továbbítják, és különösen nem gátolja meg őket abban, hogy előírják az adatátvevő számára, hogy bocsássa rendelkezésükre ezeket az adatokat. Ily módon e kérdés az ilyen adatok megfelelő védelmi szintje kizárólagosan szerződéses mechanizmusok révén történő biztosításának lehetőségét kérdőjelezi meg. A tizenegyedik kérdés általánosabb jelleggel, a Charta 7., 8. és 47. cikke fényében érinti a 2010/87 határozat érvényességét.

44 E tekintetben a GDPR (6) preambulumbekezdése azt mondja ki, hogy az adatvédelem „magas szintű” védelmét kell biztosítani mind az Unión belül, mind az azon kívülre irányuló adattovábbítás esetén. Lásd még a GDPR (101) preambulumbekezdését.

45 Lásd: Schrems ítélet (73. pont), valamint 1/15 vélemény (214. pont).

46 Ez nem sérti annak lehetőségét, hogy a személyes adatok továbbítására megfelelő garanciák hiányában is sor kerülhet a GDPR 49. cikkének (1) bekezdésében előírt eltérési okok alapján.

122. A nyolcadik kérdés arra kéri a Bíróságot, hogy állapítsa meg, hogy a felügyeleti hatóság köteles-e gyakorolni a GDPR 58. cikke (2) bekezdésének f) és j) pontjában rá ruházott hatásköröket annak érdekében, hogy felfüggessze a harmadik országba irányuló, a 2010/87 határozatban előírt általános szerződési feltételeken alapuló adattovábbítást, amennyiben úgy ítéli meg, hogy az adatátvevőt ott olyan kötelezettségek terhelik, amelyek megakadályozzák e feltételek tiszteletben tartásában, és amelyek eredményeként nem biztosított a továbbított adatok megfelelő védelme. Mivel az e kérdésre adandó válasz álláspontom szerint kihat a 2010/87 határozat [47] érvényességére, azt együtt tárgyalom a hetedik és a tizenegyedik kérdéssel.

123. A GDPR 46. cikke (1) bekezdésének szövegezése, amennyiben azt írja elő, hogy „*[a] 45. cikk (3) bekezdése szerinti határozat hiányában* az adatkezelő vagy adatfeldolgozó csak abban az esetben továbbíthat személyes adatokat harmadik országba […] ha […] megfelelő garanciákat *nyújtott* […]” (kiemelés tőlem), bemutatja a 2010/87 határozatban előírthoz hasonló szerződéses mechanizmusok által követett logikát. Amint azt a GDPR (108) és (114) preambulumbekezdése hangsúlyozza, e mechanizmusok célja az adattovábbítások lehetővé tétele azon harmadik országokba, amelyek vonatkozásában a Bizottság nem hozott megfelelőségi határozatot: ilyenkor az e harmadik ország jogrendjében biztosított védelem esetleges elégtelenségeit olyan garanciák *kompenzálják*, amelyek tiszteletben tartását az adatátadó és az adatátvevő szerződésben vállalta.

124. Mivel a szerződéses garanciák célja éppen a célországnak számító harmadik ország által nyújtott védelem bármilyen lehetséges hiányosságainak orvoslása, a Bizottság által hozott olyan határozat érvényessége, amellyel megállapítja, hogy egyes általános szerződési feltételek megfelelően pótolják e hiányosságokat, nem függhet az egyes olyan harmadik országokban biztosított védelem szintjétől, amelyekbe az adatokat esetlegesen továbbítani lehet. Az ilyen határozat érvényessége kizárólag az e kikötések által a célországnak számító harmadik ország által nyújtott védelem esetleges elégtelenségének kompenzálása céljából nyújtott garanciák erősségétől függ. E garanciák tényleges érvényesülését azon biztosítékokat is figyelembe véve kell értékelni, amelyeket a felügyeleti hatóságok GDPR 58. cikkének (2) bekezdésének alapuló hatáskörei képeznek.

125. E tekintetben, amint arra lényegében a DPC, M. Schrems, a BSA, Írország, az osztrák, a francia, a lengyel és a portugál kormány, valamint a Bizottság is rámutatott, az általános szerződési feltételekben szereplő garanciák mérsékelhetők, sőt megszüntethetők, amennyiben a célországnak számító harmadik ország az e kikötések által előírtakkal ellentétes kötelezettségeket ír elő az adatátvevő számára. Ily módon a célországnak számító harmadik országban érvényesülő jogi háttér az adattovábbítás konkrét körülményeitől függően [48] lehetetlenné teheti az e feltételek által előírt kötelezettségek teljesítését.

126. E körülmények között, amint azt M. Schrems és a Bizottság hangsúlyozta, a GDPR 46. cikke (2) bekezdésének c) pontjában előírt szerződéses mechanizmus a felelősségnek az adatátadóra, illetve másodlagosan a felügyeleti hatóságra telepítésén alapszik. Az adatkezelőnek, illetve ennek hiányában a felügyeleti hatóságnak minden konkrét adattovábbítás vonatkozásában *esetről esetre* kell megvizsgálnia, hogy a célországnak számító harmadik ország joga akadályát képezi-e az általános szerződési feltételek végrehajtásának, és ebből következően a továbbított adatok megfelelő védelmének, és hogy ily módon meg kell-e tiltani vagy fel kell-e függeszteni az adattovábbításokat.

47 Lásd a jelen indítvány 128. pontját.

48 Képzeljük el például, hogy egy harmadik ország azt a kötelezettséget írja elő a távközlési szolgáltatók számára, hogy bármilyen korlátozás és garanciák nélkül biztosítsanak hozzáférést a továbbított adatokhoz a hatóságok számára. Bár e szolgáltatók nem lennének képesek az általános szerződési feltételek tiszteletben tartására, azok a vállalkozások, amelyekre nem vonatkozik e kötelezettség, nem lennének akadályoztatva abban.

127. Ezen észrevételeket figyelembe véve úgy vélem, hogy az, hogy a 2010/87 határozat és az abban rögzített általános szerződési feltételek nem kötelezik a célországnak számító harmadik ország hatóságait, önmagában nem teszi érvénytelenné e határozatot. A 2010/87 határozat megfelelése a Charta 7., 8. és 47. cikkének álláspontom szerint attól függ, hogy léteznek-e olyan kellően erős mechanizmusok, amelyek lehetővé teszik annak biztosítását, hogy az általános szerződési feltételeken alapuló adattovábbításokat felfüggesszék vagy megtiltsák a feltételek megsértése, illetve tiszteletben tartásuk lehetetlensége esetén.

128. Ezzel kapcsolatban a GDPR 46. cikkének (1) bekezdése azt írja elő, hogy a megfelelő garanciákon alapuló adattovábbításra csak „azzal a feltétellel [kerülhet sor], hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre”. Meg kell vizsgálni, hogy a 2010/87 határozat mellékletében szereplő feltételekben előírt garanciák – a felügyeleti hatóságok hatásköreivel kiegészülve – lehetővé teszik-e ezen feltétel tiszteletben tartásának biztosítását. Álláspontom szerint ez csak akkor igaz, ha fennáll egy, az adatkezelőket (1. rész), illetve ezek tétlensége esetén a felügyeleti hatóságokat (2. rész) terhelő *kötelezettség* az adattovábbítás felfüggesztésére vagy megtiltására, amennyiben az általános szerződési feltételekből következő kötelezettségek és a célországnak számító harmadik ország joga által előírt kötelezettségek ütközése miatt az említett feltételeket nem lehet tiszteletben tartani.

1. Az adatkezelőket terhelő kötelezettségekről

129. Először is, a 2010/87 határozat mellékletében szereplő általános szerződési feltételek azt írják elő, hogy az általuk előírt kötelezettségek és a célországnak számító harmadik ország jogából következő előírások ütközése esetén az említett feltételekre nem lehet hivatkozni az e harmadik országba irányuló adattovábbítás alátámasztása érdekében, vagy pedig, ha az adattovábbítást az említett feltételek alapján már megkezdték, az adatátadót tájékoztatni kell az ütközésről és az felfüggesztheti az említett adattovábbítást.

130. Ily módon az 5. általános szerződési feltétel a) pontja alapján az adatátvevő vállalja, hogy a továbbított személyes adatokat kizárólag az adatátadó nevében kezeli, utasításainak és az általános szerződési feltételeknek megfelelően. Amennyiben az adatátvevő nem képes megfelelni ezeknek a feltételeknek, haladéktalanul tájékoztatja erről az adatátadót, aki ez esetben jogosult felfüggeszteni az adattovábbítást és/vagy a szerződéstől elállni.[49]

131. Az 5. szerződéses feltételre vonatkozó 5. lábjegyzet rögzíti, hogy az általános szerződési feltételeket nem sérti, ha az adatátvevő a rá a harmadik országban alkalmazandó nemzeti jogszabály kötelező követelményeinek tesz eleget, amennyiben e követelmények nem lépnek túl azon, amire a 95/46 irányelv 13. cikkének (1) bekezdésében (amelynek tartalmát a GDPR 23. cikkének (1) bekezdése lényegében átvette) felsorolt érdekek valamelyike alapján egy demokratikus társadalomban szükség van: ezek között szerepel a közbiztonság és a nemzetbiztonság. Ezzel szemben e feltételek figyelmen kívül hagyását a célországnak számító harmadik ország jogán alapuló olyan kötelező kötelezettségnek való megfelelés céljából, amely túlmegy az Unió által elismert jogos érdek megőrzése érdekében arányos mértéken, az említett feltételek megsértésének kell tekinteni.

49 Egyébként megjegyzem, hogy az 5. szerződéses feltétel d) pontjának i. alpontja mentesíti az adatátvevőt azon kötelezettsége alól, hogy értesítse az adatátadót a harmadik ország bűnüldöző szervének a személyes adatok közlésére irányuló jogilag kötelező erejű felhívásáról, amennyiben az ilyen értesítés a harmadik ország jogával ellentétes. Ilyen esetben az adatátadónak nincs lehetősége az adattovábbítás felfüggesztésére, amennyiben e közlés, amelyről nincsen tudomása, sérti az általános szerződési feltételeket. Ugyanakkor az 5. szerződéses feltétel a) pontja alapján az adatátvevő továbbra is köteles adott esetben tájékoztatni az adatátvevőt arról, hogy úgy véli, hogy az említett harmadik ország jogszabályai megakadályozzák abban, hogy teljesítse a kikötött általános szerződési feltételeken alapuló kötelezettségeit.

132. Álláspontom szerint, ahogy azt M. Schrems és a Bizottság is kifejti, az 5. általános szerződési feltétel a) pontját nem lehet úgy értelmezni, hogy az azt jelenti, hogy az adattovábbítás felfüggesztése vagy a szerződéstől való elállás csak lehetőség, amennyiben az adatátvevő nem képes az általános szerződési feltételek tiszteletben tartására. Bár e feltétel csak az adatátadó ilyen értelmű jogára utal, e szövegezést azon szerződéses háttér alapján kell értelmezni, amelybe az illeszkedik. Az, hogy az adatátadót *az adatátvevővel fennálló kétoldalú kapcsolataiban* felruházták az adattovábbítás felfüggesztésének vagy a szerződéstől való elállásnak a jogával, amennyiben az adatátvevő nem képes az általános szerződési feltételek tiszteletben tartására, nem hat ki az adatátadó azon kötelezettségére, hogy ily módon járjon el *az érintettek jogainak védelmére irányuló, a GDPR-ből következő kötelezettségre tekintettel*. Bármely más értelmezés a 2010/87 határozat érvénytelenségét vonná maga után, mivel az abban rögzített általános szerződési feltételek nem teszik lehetővé az adattovábbítás „megfelelő garanciákkal” való körülbástyázását, amint azt a GDPR Charta rendelkezéseinek fényében értelmezett 46. cikkének (1) bekezdése megköveteli. [50]

133. Ezenfelül az 5. általános szerződési feltétel b) pontja szerint az adatátvevő igazolja, hogy nincs tudomása arról, hogy a rá vonatkozó jogszabályok akadályoznák az adatátadótól kapott utasítások és a szerződésben vállalt kötelezettségek teljesítését. Abban az esetben, ha a jogszabályok módosítása előreláthatóan jelentősen hátrányos hatással lenne az általános szerződési feltételekben rá vonatkozóan megállapított garanciákra és kötelezettségekre, az adatátvevő azonnal köteles értesíteni a módosításról az adatátadót – ebben az esetben az adatátadó jogosult felfüggeszteni az adattovábbítást és/vagy a szerződéstől elállni. A 4. általános szerződési feltétele g) pontja szerint az adatátadó, amennyiben úgy dönt, hogy folytatja az adattovábbítást, köteles továbbítani az adatátvevőtől kapott értesítést az illetékes felügyeleti hatóság részére.

134. Álláspontom szerint itt néhány pontosítást kell tenni azon vizsgálat tartalmát illetően, amelyet a szerződés feleinek az 5. általános szerződésre vonatkozó lábjegyzetre figyelemmel annak eldöntése céljából kell elvégezniük, hogy a harmadik ország joga által az adatátvevő részére előírt kötelezettségek az általános szerződési feltételek megsértésével járnak-e, és ebből következően megakadályozzák-e azt, hogy az adattovábbítást megfelelő garanciákkal vegyék körül. E problémakört lényegében az előzetes döntéshozatalra előterjesztett hatodik kérdés második felében hozták fel.

135. Az ilyen vizsgálat álláspontom szerint az egyes adattovábbításokra jellemző valamennyi körülmény figyelembevételével jár: ezek közé tartozhat az adatok jellege és esetleges különleges volta, az adatátadó és/vagy az adatátvevő által az adattovábbítás biztonságának garantálása érdekében érvényesített mechanizmusok, [51] a harmadik ország hatóságai adatkezeléseinek jellege és célja, ezek részletszabályai, továbbá a harmadik ország által biztosított korlátozások és garanciák. A hatóságok adatkezelési tevékenységére jellemző elemek és az említett harmadik ország jogrendjében alkalmazandó garanciák álláspontom szerint átfedésben lehetnek a GDPR 45. cikkének (2) bekezdésében rögzítettekkel.

136. Másodsorban, a 2010/87 határozat mellékletében rögzített általános szerződési feltételek az adatátadóval, és másodlagosan az adatátvevővel szemben érvényesíthető jogokat, illetve jogorvoslati lehetőségeket biztosítanak az érintettek számára.

50 Az ítélkezési gyakorlatból az következik, hogy a végrehajtási aktus rendelkezéseit azon alapul szolgáló jogi aktus rendelkezéseivel összhangban kell értelmezni, amellyel a jogalkotó engedélyezte a végrehajtási aktus meghozatalát (lásd ebben az értelemben többek között: 2017. július 26-i Cseh Köztársaság kontra Bizottság ítélet [C-696/15 P, EU:C:2017:595, 51. pont]; 2018. május 17-i Evonik Degussa ítélet [C-229/17, EU:C:2018:323, 29. pont]; 2019. június 20-i ExxonMobil Production Deutschland ítélet [C-682/17, EU:C:2019:518, 112. pont]). Ezenkívül az uniós jogi aktust – amennyire lehetséges – úgy kell értelmezni, hogy ne váljon kérdésessé annak érvényessége, és hogy megfeleljen az elsődleges jog egészének, különösen a Charta rendelkezéseinek (lásd többek között: 2019. május 14-i M és társai ítélet [C-391/16, C-77/17 és C-78/17, EU:C:2019:403, 77. pont, valamint az ott hivatkozott ítélkezési gyakorlat]).

51 E tekintetben a GDPR (109) preambulumbekezdése arra ösztönzi az adatátadót és az adatátvevőt, hogy további garanciákkal egészítsék ki az általános adatvédelmi kikötéseket, többek között szerződéses úton.

137. Ily módon „A kedvezményezett harmadik személyről szóló rendelkezés” című 3. általános szerződési feltétel (1) bekezdése jogorvoslati jogot biztosít az adatátadóval szemben, többek között az 5. általános szerződési feltétel a) vagy b) pontjának megsértése esetén. A 3. általános szerződési feltétel (2) bekezdése szerint, amennyiben az adatátadó vállalkozása ténylegesen vagy jogilag megszűnik létezni, az érintett az adatátvevővel szemben érvényesítheti ezt az általános szerződési feltételt.

138. A 6. általános szerződési feltétel (1) bekezdése szerint az érintett, aki a 3. általános szerződési feltételben említett kötelezettségek megsértésének következményeként kárt szenved, kártérítésre jogosult az adatátadótól. A 7. általános szerződési feltétel (1) bekezdése alapján az adatátvevő vállalja, hogy amennyiben az érintett érvényesíteni kívánja vele szemben a kedvezményezett harmadik személy jogait, és/vagy az általános szerződési feltételek alapján követeli a károk megtérítését, elfogadja az érintett azon döntését, hogy a jogvitával közvetítés céljából egy független személyhez vagy adott esetben a felügyeleti hatósághoz fordul, illetve hogy a jogvitával az adatátadó letelepedési helye szerinti tagállam bíróságához fordul.

139. A 2010/87 határozat mellékletében szereplő általános szerződési feltételek alapján őket megillető jogorvoslati lehetőségek mellett az érintett személyek, amennyiben úgy vélik, hogy e feltételeket megsértették, a felügyeleti hatóságoktól a 2010/87 határozat 4. cikkében hivatkozott GDPR 58. cikkének (2) bekezdése alapján korrekciós intézkedések meghozatalát kérhetik.[52]

2. A felügyeleti hatóságokat terhelő kötelezettségekről

140. Az alábbi okok miatt M. Schrems-hez, Írországhoz, a német, az osztrák, a belga, a holland és a portugál kormányhoz, valamint az EDPB-hez hasonlóan úgy vélem, hogy a GDPR 58. cikkének (2) bekezdése arra kötelezi a felügyeleti hatóságot, amennyiben gondos vizsgálat eredményeként úgy véli, hogy a harmadik országba továbbított adatok a kikötött általános szerződési feltételek tiszteletben tartásának elmaradása miatt nem részesülnek megfelelő védelemben, hogy hozzon megfelelő intézkedéseket a jogellenesség orvoslása céljából, szükséges esetén elrendelve az adattovábbítás felfüggesztését.

141. Elsőként megjegyzem, hogy a DPC által előadottakkal ellentétben a 2010/87 határozat egyetlen rendelkezése sem korlátozza kivételes esetekre a felügyeleti hatóságokat a GDPR 58. cikke (2) bekezdésének f) és j) pontja alapján megillető azon hatáskörök gyakorlását, hogy „átmenetileg vagy véglegesen korlátozz[ák] az adatkezelést, ideértve az adatkezelés megtiltását is”, illetve hogy „[elrendeljék] a harmadik országbeli címzett vagy nemzetközi szervezet felé irányuló adatáramlás felfüggesztését”.

142. A 2010/87 határozat 4. cikke (1) bekezdésének eredeti szövege vitathatatlanul a határokon átnyúló adatáramlások felfüggesztésére vagy megtiltására korlátozta a felügyeleti hatóságok hatásköreit egyes olyan esetekben, amikor bizonyítást nyert, hogy a szerződéses feltételeken alapuló adattovábbítás jelentősen hátrányos hatással lehet az érintett védelmét szolgáló garanciákra. Ugyanakkor e határozat 4. cikke, amelyet a Bizottság 2016-ban a Schrems ítéletnek való megfelelés céljából módosított,[53] immár pusztán utal e hatáskörökre, anélkül hogy azokat bármilyen módon korlátozná. Mindenesetre a 2010/87 határozathoz hasonló bizottsági végrehajtási határozat nem korlátozhatja érvényesen a GDPR által a felügyeleti hatóságokra ruházott hatásköröket.[54]

52 Bár a 2010/87 határozat 4. cikkének (1) bekezdése a 95/46 irányelv 28. cikkének (3) bekezdésére hivatkozik, megismétlem, hogy a GDPR 94. cikkének (2) bekezdése alapján az említett irányelvre való hivatkozásokat úgy kell értelmezni, mint amelyek a GDPR megfelelő rendelkezéseire utalnak.

53 Lásd a 2016/2297 határozat (6) és (7) preambulumbekezdését. A Schrems ítélet 101–104. pontjában a Bíróság érvénytelennek nyilvánította a „biztonságos kikötő” határozat egy olyan rendelkezését, amely „kivételes esetekre” korlátozta a 95/46 irányelv 28. cikke által a felügyeleti hatóságokra ruházott hatásköröket, azzal az indokkal, hogy a Bizottságnak nincs hatásköre e hatáskörök korlátozására.

54 Lásd: Schrems ítélet (103. pont).

143. E következtetést nem kérdőjelezi meg a 2010/87 határozat (11) preambulumbekezdése, amely szerint a felügyeleti hatóságok az adattovábbítások felfüggesztésére és megtiltására irányuló hatásköröket csak „kivételes esetekben” gyakorolhatják. Ez a – már a határozat eredeti változatában is meglevő – preambulumbekezdés az említett határozat korábbi 4. cikkének (1) bekezdésére vonatkozik, amely korlátozta a felügyeleti hatóságok hatásköreit. A 2010/87 határozatnak a 2016/2297 határozattal történő felülvizsgálata során a Bizottság elmulasztotta az említett preambulumbekezdés hatályon kívül helyezését vagy módosítását annak érdekében, hogy tartalmát az új 4. cikkben előírtakhoz igazítsa. A 2016/2297 határozat (5) preambulumbekezdése ugyanakkor megerősítette a felügyeleti hatóságok hatáskörét az általuk az uniós joggal ellentétesnek ítélt bármely adattovábbítás többek között amiatt történő felfüggesztésére vagy betiltására, hogy az adatátvevő nem tartja tiszteletben az általános szerződési feltételeket. A 2010/87 határozat (11) preambulumbekezdését elavultnak kell tekinteni, mivel immár ellentmond a határozat egy jogilag kötelező rendelkezése szövegének és céljának is. [55]

144. Másodsorban, ellentétben a DPC által előadottakkal, a GDPR 58. cikke (2) bekezdésének f) és j) pontjában előírt felfüggesztési és megtiltási hatáskör immár nem a felügyeleti hatóságok mérlegelésére bízott puszta lehetőség. E megállapítás következik álláspontom szerint a GDPR 58. cikke (2) bekezdésének e rendelet más rendelkezései és a Charta fényében végzett értelmezéséből, valamint a 2010/87 határozat általános rendszeréből és céljaiból.

145. Közelebbről, a GDPR 58. cikkének (2) bekezdését a Charta 8. cikke (3) bekezdésének, valamint az EUMSZ 16. cikk (2) bekezdésének fényében kell értelmezni. E rendelkezéseknek megfelelően a személyes adatok védelméhez való alapvető joggal járó követelmények tiszteletben tartását független hatóságok ellenőrzik. Ezen, a személyes adatok védelmével kapcsolatos követelmények tiszteletben tartásával kapcsolatos felügyeleti feladat, amely a GDPR 57. cikke (1) bekezdésének a) pontjában is szerepel, a felügyeleti hatóságok arra irányuló kötelezettségével jár, hogy az e rendelet megfelelő alkalmazását biztosító módon járjanak el.

146. Ily módon a felügyeleti hatóságnak kellő gondossággal meg kell vizsgálnia az azon személy által benyújtott panaszt, akinek adatait állítólagosan az adattovábbításra alkalmazandó általános szerződési feltételeket megsértve továbbították harmadik országba. [56] A GDPR 58. cikkének (1) bekezdése ennek érdekében jelentős vizsgálati hatáskörökkel ruházza fel a felügyeleti hatóságokat. [57]

147. Az illetékes felügyeleti hatóság köteles továbbá megfelelően reagálni az érintett jogainak az általa folytatott vizsgálat eredményeként megállapított esetleges megsértéseire. E tekintetben a GDPR 58. cikkének (2) bekezdése alapján minden felügyeleti hatóság az eszközök széles skálájával – a korrekciós intézkedések elfogadására irányuló, e rendelkezésben felsorolt hatáskörökkel – rendelkezik, a rá háruló feladat ellátása érdekében. [58]

148. Noha a leghatékonyabb módszernek a szóban forgó adattovábbítás összes körülményére figyelemmel történő kiválasztása az illetékes felügyeleti hatóság mérlegelési jogkörébe tartozik, e hatóság köteles teljes mértékben ellátni a rábízott felügyeleti feladatot. Adott esetben e hatóságnak fel kell függesztenie az adattovábbítást, ha azt állapítja meg, hogy nem tartották tiszteletben az általános szerződési feltételeket, és hogy a továbbított adatok megfelelő védelme, azon kívül, hogy az adatátadó megszünteti az adattovábbítást, más eszközzel nem biztosítható.

55 Mindenesetre az uniós jogi aktus preambulumának nincs kötelező jogi ereje és arra nem lehet hivatkozni az ugyanezen aktus rendelkezéseitől való eltérés érdekében. Lásd: 1998. november 19-i Nilsson és társai ítélet (C-162/97, EU:C:1998:554, 54. pont); 2005. május 12-i Meta Fackler ítélet (C-444/03, EU:C:2005:288, 25. pont); 2006. január 10-i IATA és ELFAA ítélet (C-344/04, EU:C:2006:10, 76. pont).

56 Lásd analógia útján: Schrems ítélet (63. pont).

57 Ehhez hozzáteszem, hogy a 2010/87 határozat mellékletében található 8. általános szerződési feltétel (2) bekezdése szerint a szerződés felei megállapodnak abban, hogy a felügyeleti hatóság számára hatáskört biztosítanak arra, hogy ugyanolyan feltételek mellett végezzen ellenőrzéseket az adatátvevőnél, mint az alkalmazandó jog alapján az adatátadónál végzendő ellenőrzések esetében.

58 Lásd ebben az értelemben: Schrems ítélet (43. pont).

149. Ezt az értelmezést megerősíti a GDPR 58. cikkének (4) bekezdése is, amely azt írja elő, hogy e cikk alapján a felügyeleti hatóságra ruházott hatáskörök gyakorlására megfelelő garanciák mellett kerülhet sor, ideértve a Charta 47. cikkének megfelelően a hatékony bírósági jogorvoslathoz való jogot is. A GDPR 78. cikkének (1) és (2) bekezdése egyébként elismeri minden személy jogát a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben, illetve ha a felügyeleti hatóság elmulasztja panasz kivizsgálását.[59]

150. E rendelkezések eredményeként, amint azt lényegében M. Schrems, a BSA, Írország, a lengyel kormány és az Egyesült Királyság kormánya, valamint a Bizottság kifejti, bírósági felülvizsgálat tárgyát képezheti az a határozat, amely révén a felügyeleti hatóság tartózkodik attól, hogy egy olyan személy kérelmére megtiltson vagy felfüggesszen egy harmadik országba irányuló adattovábbítást, aki annak veszélyére hivatkozik, hogy a rá vonatkozó adatokat alapvető jogaival ellentétes módon fogják kezelni. Márpedig a bírósági jogorvoslathoz való jog elismerése feltételezi a felügyeleti hatóságok kötött, nem tisztán diszkrecionális jogkörének fennállását. Ezenkívül M. Schrems és a Bizottság megalapozottan hangsúlyozták, hogy a hatékony bírósági felülvizsgálat gyakorlása azt igényli, hogy a vitatott aktust kiadó hatóság megfelelően indokolja meg azt.[60] Ezen indokolási kötelezettség álláspontom szerint kiterjed a felügyeleti hatóságok részéről a GDPR 58. cikkének (2) bekezdése által rájuk ruházott hatáskörök közül annak kiválasztására is, amelyet gyakorolni fognak.

151. Ugyanakkor még meg kell válaszolni azokat az érveket, amelyekben a DPC előadja, hogy bár a felügyeleti hatóságok kötelesek felfüggeszteni vagy megtiltani az adattovábbítást, ha az érintett jogainak védelme ezt igényli, a 2010/87 határozat érvényessége azonban ettől még nem biztosított.

152. Először, a DPC úgy véli, hogy az ilyen kötelezettség nem orvosolja az Egyesült Államokhoz hasonló országokban a megfelelő garanciák hiányához kapcsolódó, rendszerszintű problémákat. A felügyeleti hatóságok hatásköreit ugyanis csak esetről esetre lehet gyakorolni, miközben az amerikai jogra jellemző hiányosságok általános és szerkezeti jellegűek. Ebből annak a veszélye következik, hogy a különböző felügyeleti hatóságok eltérő határozatokat fogadnak el összehasonlítható adattovábbítások vonatkozásában.

153. E kérdést illetően nem lehet figyelmen kívül hagyni az azon jogalkotói döntéshez kapcsolódó gyakorlati nehézségeket, hogy a felügyeleti hatóságokra telepítik annak felelősségét, hogy gondoskodjanak az érintettek alapvető jogainak tiszteletben tartásáról a konkrét adattovábbítások, illetve az adott címzett felé tartó adatáramlások során. E nehézségek álláspontom szerint ugyanakkor nem vonják maguk után a 2010/87 határozat érvénytelenségét.

154. Az uniós jog ugyanis véleményem szerint nem követeli meg azt, hogy átfogó és preventív megoldás szülessen egy adott harmadik országba irányuló valamennyi olyan adattovábbítás vonatkozásában, amely az alapvető jogok megsértésének ugyanolyan veszélyét hordozza.

155. Ezenfelül a különböző felügyeleti hatóságok által követett megközelítések töredezettségének kockázata elválaszthatatlan a jogalkotó által elérni kívánt decentralizált felügyeleti struktúrától.[61] Mindemellett, amint azt a német kormány kiemelte, a GDPR „Együttműködés és egységesség” című VII. fejezete e veszély elkerülését célzó mechanizmusokat alakít ki. E rendelet 60. cikke határokon

59 A GDPR (141) preambulumbekezdésének megfogalmazása szerint minden személy jogosult arra, hogy a Charta 47. cikkével összhangban hatékony bírósági jogorvoslattal éljen, ha úgy ítéli meg, hogy a felügyeleti hatóság „nem jár el olyan esetben, amikor fellépése [e személy] jogainak védelmében szükséges lenne”. Lásd még a GDPR (129) és (143) preambulumbekezdését.

60 Lásd többek között: 2011. július 28-i Samba Diouf ítélet (C-69/10, EU:C:2011:524, 57. pont); 2011. november 17-i Gaydarov ítélet (C-430/10, EU:C:2011:749, 41. pont).

61 Lásd ezzel kapcsolatban: 2018. június 5-i Wirtschaftsakademie Schleswig-Holstein ítélet (C-210/16, EU:C:2018:388, 69–73. pont).

átnyúló adatkezelés esetén az érintett felügyeleti hatóságok és az adatkezelő tevékenységi központja szerinti felügyeleti hatóság – a „fő felügyeleti hatóság” – közötti együttműködési eljárást ír elő.[62] Eltérő vélemények esetén a vitát az EDPB dönti el.[63] E testület arra is hatáskörrel rendelkezik, hogy egy felügyeleti hatóság kérelmére több tagállamot érintő véleményt bocsásson ki.[64]

156. Másodszor a DPC arra hivatkozik, hogy a 2010/87 határozat a Charta 47. cikkére figyelemmel, azzal az indokkal érvénytelen, hogy a felügyeleti hatóságok csak a jövőre nézve védhetik meg az érintettek jogait, anélkül hogy megoldást kínálhatnának azon érintettek számára, akiknek adatait már továbbították. Közelebbről a DPC rámutat, hogy a GDPR 58. cikkének (2) bekezdése nem ír elő hozzáférési, helyesbítési vagy törlési jogot a harmadik országbeli hatóságok által gyűjtött adatok vonatkozásában, ahogy az érintettek által elszenvedett károk megtérítésének lehetőségét sem.

157. A gyűjtött adatokkal kapcsolatos hozzáférési, helyesbítési vagy törlési jog állítólagos hiányát illetően meg kell állapítani, hogy amennyiben semmilyen hatékony jogorvoslat nem áll fenn a célországnak számító harmadik országban, az Unión belül az adatkezelővel szemben előírt jogorvoslatok nem teszik lehetővé annak elérését, hogy az említett harmadik ország hatóságai hozzáférést biztosítsanak ezen adatokhoz, illetve helyesbítsék vagy töröljék azokat.

158. Álláspontom szerint e kifogás ugyanakkor nem igazolja a 2010/87 határozatnak a Charta 47. cikkével való összeegyeztethetetlenségét. E határozat érvényessége ugyanis nem az egyes, olyan harmadik országokban fennálló védelmi szinttől függ, amelybe az adatokat a határozatban rögzített általános szerződési feltételek alapján továbbítani lehetne. Ha a célországnak számító harmadik ország joga megakadályozza, hogy az adatátvevő tiszteletben tartsa e feltételeket, előírva számára, hogy anélkül biztosítson hozzáférést az adatokhoz, hogy ehhez megfelelő jogorvoslati lehetőségeket biztosítana, a felügyeleti hatóságoknak kell korrekciós intézkedéseket hozniuk, amennyiben az adatátadó a 2010/87 határozat mellékletében szereplő 5. általános kikötés a) vagy b) pontja alapján nem függesztette fel az adattovábbítást.

159. Egyebekben, amint azt M. Schrems hangsúlyozza, azon személyeket, akiknek jogait megsértették, a GDPR 82. cikke alapján immár megilleti az e rendelet megsértésének eredményeként elszenvedett vagyoni vagy nem vagyoni kár megtérítésének joga az adatkezelővel vagy az adatfeldolgozóval szemben.[65]

160. Amint az a fenti megfontolások összességéből következik, elemzésem során nem derült fény olyan körülményre, amely kihathatna a 2010/87 határozat érvényességére a Charta 7., 8. és 47. cikkének fényében.

F. Arról, hogy nem kell válaszolni az előzetes döntéshozatalra előterjesztett egyéb kérdésekre, illetve nem kell megvizsgálni az adatvédelmi pajzsról szóló határozat érvényességét

161. A jelen részben kifejtem azokat az elsődlegesen az alapeljárás tárgyának a 2010/87 határozat érvényességére korlátozásával kapcsolatos okokat, amelyek miatt úgy vélem, hogy nem kell megválaszolni az előzetes döntéshozatalra előterjesztett második, harmadik, negyedik, ötödik, valamint kilencedik és tizedik kérdést, valamint nem kell dönteni az adatvédelmi pajzsról szóló határozat érvényességéről.

62 Lásd a GDPR 56. cikkének (1) bekezdését. E rendelet 61. cikke szerint a felügyeleti hatóságok kölcsönösen segítséget nyújtanak egymásnak. Az említett rendelet 62. cikke felhatalmazza őket közös műveletek végrehajtására.

63 Lásd a GDPR 65. cikkét.

64 Lásd a GDPR 64. cikkének (2) bekezdését.

65 A GDPR 83. cikke (5) bekezdésének c) pontja az adatkezelőt terhelő bírságokat is előír e rendelet 44–49. cikkének megsértése esetén.

162. Az előzetes döntéshozatalra előterjesztett második kérdés azon védelmi előírások azonosításával kapcsolatos, amelyeket a harmadik országnak tiszteletben kell tartania ahhoz, hogy az adatokat jogszerűen továbbítani lehessen oda az általános szerződési feltételek alapján, amennyiben elképzelhető, hogy ezeket az adatokat a továbbításukat követően az említett harmadik ország hatóságai nemzetbiztonsági célokra használják fel. A Bíróság elé terjesztett harmadik kérdés a célországnak számító harmadik országban alkalmazandó védelmi rendszerre jellemző azon körülmények meghatározásra vonatkozik, amelyeket figyelembe kell venni annak ellenőrzése során, hogy ezen ország megfelel-e az említett előírásoknak.

163. Negyedik, ötödik és hatodik kérdésével a kérdést előterjesztő bíróság lényegében azt kívánja megtudni, hogy figyelemmel az általa az Egyesült Államok jogát illetően megállapított tényekre, abban megfelelő garanciákat írnak-e elő az amerikai hírszerzési hatóságok beavatkozásaival szemben az olyan alapvető jogok gyakorlását illetően, mint a magánélet tiszteletben tartása, a személyes adatok védelme és a hatékony bírói jogvédelem.

164. Az előzetes döntéshozatalra előterjesztett kilencedik kérdés arra vonatkozik, hogy a felügyeleti hatóság által annak ellenőrzése érdekében folyatott vizsgálat során, hogy egy, az Egyesült Államokba irányuló, a 2010/87 határozatban előírt általános szerződési feltételeken alapuló adattovábbításhoz megfelelő garanciák kapcsolódnak-e, milyen jelentősége van annak a körülménynek, hogy a Bizottság az adatvédelmi pajzsról szóló határozatban azt állapította meg, hogy az Egyesült Államok megfelelő védelmi szintet biztosít az érintett személyek alapvető jogai tekintetében az ilyen beavatkozásokkal szemben.

165. Az adatvédelmi pajzsról szóló határozat érvényességével kapcsolatos kérdést kifejezetten nem tette fel a kérdést előterjesztő bíróság – noha amint azt a fentiekben kifejtettem,[66] az előzetes döntéshozatalra előterjesztett negyedik, ötödik és hatodik kérdés közvetve azon megfelelőségi megállapítás megalapozottságát kérdőjelezi meg, amelyet a Bizottság e határozatban tett.

166. Álláspontom szerint a fenti elemzésből következő körülményekre figyelemmel a Bíróság e kérdésekkel kapcsolatos felvilágosítása nem hathat ki a 2010/87 határozat absztrakt érvényességével kapcsolatos megállapítására, és így nem befolyásolhatja az alapeljárás kimenetelét sem (1. rész). Egyebekben, noha a Bíróság által az említett kérdésekre adandó válaszok egy későbbi szakaszban hasznosak lehetnének a DPC számára abból a célból, hogy a jelen jogvita mögötti eljárás keretében eldöntse, hogy a szóban forgó adattovábbításokat konkrétan fel kell-e függeszteni a megfelelő garanciák állítólagos hiánya miatt, álláspontom szerint korai lenne ezek eldöntése a jelen ügy során (2. rész).

1. A Bíróság válaszainak szükségtelenségéről az alapeljárás tárgya tekintetében

167. Emlékeztetek arra, hogy az alapeljárás abból ered, hogy a DPC élt a Schrems ítélet 65. pontjában ismertetett jogorvoslati lehetőséggel; e pont szerint minden tagállamnak lehetővé kell tennie a felügyeleti hatóság számára, hogy amikor szükségesnek ítéli azt az elé terjesztett panasz elbírálása céljából, felhívja a nemzeti bíróságot arra, hogy a megfelelőségi határozat – illetve analógia útján az általános szerződési feltételeket bevezető határozat – érvényességével kapcsolatban előzetes döntéshozatalra előterjesztett kérdést nyújtson be a Bírósághoz.

66 Lásd a jelen indítvány 175. pontját.

168. E tekintetben a High Court (felsőbíróság) hangsúlyozta, hogy a DPC kérelmét követően kizárólag két lehetősége volt: a 2010/87 határozat érvényességével kapcsolatos, a DPC által kért előzetes döntéshozatalra utalás kezdeményezése, amennyiben osztja az e határozat érvényességével kapcsolatos kétségeket, vagy pedig ellenkező esetben e kérelem elutasítása. E bíróság úgy véli, hogy amennyiben a második lehetőség mellett döntött volna, akkor meg kellett volna tagadnia az eljárást, mivel a DPC panaszának nem volt más tárgya. [67]

169. Ehhez hasonlóan a Facebook Ireland által az előzetes döntéshozatalra utaló határozat ellen benyújtott fellebbezés ügyében eljáró Supreme Court (legfelsőbb bíróság, Írország) úgy ismertette az alapeljárást, mint egy olyan deklaratív eljárást, amely révén a DPC azt kéri a kérdést előterjesztő bíróságtól, hogy előzetes döntéshozatal céljából terjesszen a 2010/87 határozat érvényességével kapcsolatos kérdést a Bíróság elé. Az ír legfőbb bírói szerv szerint a kérdést előterjesztő bíróság és a Bíróság előtt felmerülő egyetlen lényeges kérdés tehát e határozat érvényességét érinti. [68]

170. Tekintettel az alapeljárás ily módon körülhatárolt tárgyára, a kérdést előterjesztő bíróság a Bíróság elé terjesztette első tíz kérdését, mivel úgy ítélte meg, hogy ezek vizsgálata hozzájárulna ahhoz az átfogó vizsgálathoz, amelyet a Bíróságnak a tizenegyedik, a 2010/87 határozatnak a Charta 7., 8. és 47. cikke tekintetében való érvényességével kapcsolatos kérdés eldöntése céljából kell elvégeznie. E kérdés az előzetes döntéshozatalra utaló határozat megfogalmazása szerint az azt megelőző kérdések logikus következményét képezi.

171. Ebből a szempontból a második, harmadik, negyedik, ötödik, illetve a kilencedik és tizedik kérdést álláspontom szerint az az előfeltevés támasztja alá, amely szerint a 2010/87 határozat érvényessége az alapvető jogok azon harmadik országokban előírt védelmi szintjétől függ, amelyekbe az adatokat a határozat által előírt általános szerződési feltételek alapján továbbíthatók. Márpedig a hetedik kérdéssel kapcsolatos elemzésemből kitűnik, [69] hogy ez az előfeltevés álláspontom szerint téves. A célországnak számító harmadik ország jogának vizsgálata csak akkor releváns, ha a Bizottság megfelelőségi határozatot hoz, vagy ha az adatkezelő – vagy ennek hiányában az illetékes felügyeleti hatóság – megvizsgálja, hogy a GDPR 46. cikke (1) bekezdésének értelmében vett megfelelő garanciákon alapuló adattovábbítás során az említett harmadik ország joga által az adatátvevő számára előírt kötelezettségek nem veszélyeztetik-e az e garanciák által biztosított védelem tényleges érvényesülését.

172. Következésképpen a Bíróság fent hivatkozott kérdésekre adott válaszai nem hathatnak ki a tizenegyedik kérdéssel kapcsolatos következtetésére. [70] Így tehát azokat az alapeljárás tárgya szempontjából nem kell megválaszolni.

173. Azt javaslom a Bíróságnak, hogy a jelen ügyet e jogvita tárgyára szorítkozva bírálja el. A Bíróság álláspontom szerint nem léphet túl azon, amit az említett jogvita eldöntése igényel, az előzetes döntéshozatalra előterjesztett kérdéseknek a DPC előtt folyamatban lévő mögöttes eljárás szempontjából történő taglalása révén. Amint azt az alábbiakban kifejtem, e visszafogottságra való felhívás egyrészt azon törekvésből fakad, hogy ne kerüljük meg azon eljárás rendes lefolyását,

67 A High Court (felsőbíróság) 2017. október 3-i ítélete (337. pont).

68 A Supreme Court (legfelsőbb bíróság) 2019. május 31-i ítélete (2.7 pont) szerint „[t]he sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [TFUE]”. Ezen ítélet 2.9 pontjában a következő szerepel: „Here, the only issue of substance which arises before either the Irish courts or the CJEU is the question of the validity or otherwise of Union measures. Whatever the view taken by the CJEU on that issue, *the Irish courts will have no further role, for the measures under question will either be found to be valid or invalid and in either event, that will be the end of the matter*” (kiemelés tőlem).

69 Lásd a jelen indítvány 124. pontját.

70 Ugyanezen ok miatt a Supreme Court (legfelsőbb bíróság) 2019. május 31-i ítéletében (8.1–8.5 pont), megállapítva hatásköre hiányát a kérdést előterjesztő bíróság azon határozatának megkérdőjelezésre, amellyel az a Bíróság elé terjesztette az előzetes döntéshozatalra előterjesztett kérdéseket, valamint annak módosítására, kifejezte kétségeit egyes kérdések szükségességét illetően. Ezen ítélet 8.5 pontja konkrétan a következőket mondja ki: „The sole purpose of the proceedings before the courts in Ireland was to enable the High Court to refer that question of validity to the CJEU and obtain a definitive answer from the only court which has competence to make the decision in question. It is difficult, therefore, to see how the High Court needs answers to many of the questions which have been referred, for the answers to those questions are only relevant to the question of the validity of the challenged measures […].”

amelynek a DPC előtt kell folytatódnia, miután a Bíróság döntött a 2010/87 határozat érvényességét illetően. Másrészt a jelen ügy tényállására figyelemmel álláspontom szerint némileg elsietett lenne még ezen eljárás eredménye szempontjából is, ha a Bíróság megvizsgálná a második, harmadik, negyedik, ötödik, illetve a kilencedik és tizedik kérdésben felvetett problémaköröket.

2. Az az ellen szóló indokokról, hogy a Bíróság vizsgálatot végezzen a DPC előtt folyamatban levő eljárás tárgyát illetően

174. A DPC-hez benyújtott panaszában M. Schrems azt kéri e felügyeleti hatóságtól, hogy gyakorolja a GDPR 58. cikke (2) bekezdésének f) pontja alapján őt megillető hatáskört, és kötelezze a Facebook Irelandet arra, hogy függessze fel személyes adatai Egyesült Államokba irányuló, szerződéses feltételeken alapuló továbbítását. E kérelem alátámasztására M. Schrems lényegében az alapvető jogainak gyakorlásába való, az amerikai hírszerző szolgálatok tevékenységéből következő beavatkozásokkal kapcsolatos szerződéses garanciák nem megfelelő jellegére hivatkozik.

175. M. Schrems érvelése azt a Bizottság által az adatvédelmi pajzsról szóló határozatban rögzített megállapítást kérdőjelezi meg, amely szerint az Egyesült Államok megfelelő szintű védelmet biztosít az e határozat alapján továbbított adatok tekintetében, figyelemmel az ezen adatokhoz való hozzáférést, illetve az amerikai hírszerző szolgálatok általi felhasználásukat érintő korlátozásokra, valamint az érintettek számára biztosított jogvédelemre.[71] A DPC által ideiglenes jelleggel kifejtett, illetve a kérdést előterjesztő bíróság által negyedik, ötödik és tizedik kérdésében ismertetett aggodalmak[72] közvetve szintén e megállapodással kapcsolatos kétségeket rögzítenek.

176. Kétségtelen, hogy az adatvédelmi pajzsról szóló határozat az abban rögzített elveknek megfelelően az Egyesült Államokban székhellyel rendelkező, az említett határozatban rögzített elvekhez csatlakozásról öntanúsítással rendelkező vállalkozások számára továbbított személyes adatok védelmi szintje megfelelőségének megállapítására szorítkozik.[73] Az e határozatban szereplő megállapítások ugyanakkor túllépnek az e határozat hatálya alá tartozó adattovábbítások összefüggésén, amennyiben a továbbított adatok nemzetbiztonsági célú kezelését illetően az e harmadik országban hatályos jogra és gyakorlatra vonatkoznak. Amint azt a Facebook Ireland, M. Schrems, az Egyesült Államok kormánya és a Bizottság lényegében megjegyezte, az amerikai hírszerzési hatóságok által folytatott megfigyelés, valamint az azzal járó visszaélési kockázatok elleni garanciák, illetve az ezek tiszteletben tartásának ellenőrzését szolgáló mechanizmusok az uniós jog szempontjából az adattovábbítás alátámasztása céljából hivatkozott jogalaptól függetlenül alkalmazandók.

177. Ebből a szempontból az a kérdés, hogy az e tárgyban az adatvédelmi pajzsról szóló határozatban tett megállapítások kötelezik-e a felügyeleti hatóságokat, amikor egy olyan általános szerződési feltételeken alapuló adattovábbítás jogszerűségét vizsgálják, amely releváns lehet M. Schrems panaszának a DPC általi elbírálása tekintetében. Az e kérdésre adandó igenlő válasz esetén az a kérdés merül fel, hogy érvényes-e ez a határozat.

71 Lásd az adatvédelmi pajzsról szóló határozat (64)–(141) preambulumbekezdését. Emlékeztetek arra, amint az e határozat 1. cikkének (2) bekezdéséből is kitűnik, hogy az adatvédelmi pajzs nem csak azon elvekből áll, amelyekhez az említett határozat alapján adatokat továbbítani kívánó vállalkozásoknak csatlakozniuk kell, hanem az Egyesült Államok kormányától kapott, a határozathoz csatolt dokumentumokban szereplő hivatalos nyilatkozatokból és kötelezettségvállalásokból is.

72 A DPC határozattervezete megelőzte az adatvédelmi pajzsról szóló határozat elfogadását. Amint azt a DPC e tervezetben kimondta, noha ideiglenesen azt állapította meg, hogy az Egyesült Államok joga által előírt garanciák nem tették lehetővé legalább annak biztosítását, hogy ezek az e harmadik országba irányuló adattovábbítások megfeleljenek a Charta 47. cikkének, e szakaszban nem vizsgálta, illetve vette figyelembe az adatvédelmi pajzsról szóló egyezmény tervezetében szereplő új megállapodásokat, mivel azt még nem fogadták el. Ezt követően, 2017. október 3-i ítéletének 307. pontjában a High Court (felsőbíróság) a következőket állapítja meg: „It is fair to conclude […] that the decision of the Commission in regard to the adequacy of the protections afforded to EU citizens against interference by the intelligence authorities in the [U. S.] with the fundamental rights of EU citizens whose data are transferred from the [EU] to the [U. S.], conflicts with the case made by the DPC to this court".

73 Lásd az adatvédelmi pajzsról szóló határozat 1. cikkének (1) és (3) bekezdését, valamint (14)–(16) preambulumbekezdését.

178. Nem tanácsolom ugyanakkor a Bíróság számára, hogy kizárólag annak érdekében döntsön e kérdésekről, hogy segítséget nyújtson a DPC számára e panasz elbírálásához, noha nincs helye abból a célból megválaszolni a kérdéseket, hogy lehetővé tegyék a kérdést előterjesztő bíróság számára az alapeljárásbeli döntéshozatalt. Mivel az EUMSZ 267. cikkben előírt eljárás a bíróságok közötti párbeszédet alakít ki, a Bíróságnak nem kell felvilágosítást adnia kizárólag abból a célból, hogy segítséget nyújtson egy közigazgatási hatóság számára az e jogvita mögött meghúzódó eljárással összefüggésben.

179. A tartózkodás álláspontom szerint annál is inkább indokolt, mivel az adatvédelmi pajzsról szóló határozat érvényességének kérdését kifejezetten nem terjesztették a Bíróság elé – e határozat egyébként már megsemmisítés iránti kereset tárgya az Európai Unió Törvényszéke előtt.[74]

180. Ezenfelül a fent ismertetett problémák eldöntése esetén a Bíróság álláspontom szerint megzavarná azon eljárás rendes menetét, amelynek a jelen ügyben hozott ítélet követően kell lezajlania. Ezen eljárás során a DPC-nek a Bíróság által az előzetes döntéshozatalra előterjesztett tizenegyedik kérdésre adott válasz figyelembevételével kell elbírálnia M. Schrems panaszát. Amennyiben a Bíróság javaslatomnak megfelelően és a DPC által előadottakkal ellentétben úgy dönt, hogy a 2010/87 határozat nem érvénytelen a Charta 7., 8. és 47. cikkére tekintettel, úgy a DPC-nek álláspontom szerint lehetőséget kell biztosítani az előtte folyó eljárás iratainak ismételt vizsgálatára. Amennyiben a DPC úgy véli, hogy nem tudja elbírálni M. Schrems panaszát anélkül, hogy a Bíróság előzetesen ne döntené el, hogy az adatvédelmi pajzsról szóló határozat akadályát képezi-e a szóban forgó adattovábbítás felfüggesztésével kapcsolatos hatáskörei gyakorlásának, és kétségei lennének e határozat érvényességét illetően, akkor ismét megkeresheti a nemzeti bíróságokat annak érdekében, hogy azok ezzel kapcsolatban intézzenek kérdést a Bírósághoz.[75]

181. Ebben az esetben olyan eljárás kezdődne, amely a Bíróság alapokmánya 23. cikkének második bekezdésében hivatkozott valamennyi fél és érdekelt számára lehetővé teszi, hogy észrevételeket tegyen kifejezetten az adatvédelmi pajzsról szóló határozat érvényességét illetően, feltüntetve adott esetben az általa vitatott, konkrét értékeléseket, valamint azokat az okokat, amelyek miatt úgy véli, hogy a Bizottság túllépett a rendelkezésére álló korlátozott mérlegelési mozgástéren.[76] Egy ilyen eljárás során a Bizottságnak lehetősége lenne arra, hogy konkrétan és részletesen választ adjon az említett határozattal szemben felhozott valamennyi esetleges kifogásra. Noha a jelen ügy lehetőséget nyújtott a felek és a Bíróság elé észrevételt terjesztő érdekeltek számára egyes, az adatvédelmi pajzsról szóló határozat Charta 7., 8. és 47. cikkének való megfelelését illetően releváns szempontok megvitatására, e kérdés, tárgyára figyelemmel, kimerítő és alapos vitát igényel.

182. Álláspontom szerint az óvatosság azt követeli meg, hogy várjuk meg, amíg ezen eljárási szakaszokra sor kerül, mielőtt a Bíróság megvizsgálná azt a hatást, amelyet az adatvédelmi pajzsról szóló határozat gyakorol az Egyesült Államokba irányuló, a GDPR 46. cikkének (1) bekezdése alapján végzett adattovábbítás felfüggesztése iránti kérelem felügyeleti hatóság általi elbírálására, és döntene e határozat érvényességéről.

183. Annál is inkább ez a helyzet, mivel a Bíróság elé terjesztett iratok alapján nem állapítható meg, hogy M. Schrems panaszának a DPC általi elbírálása szükségszerűen attól függ, hogy az adatvédelmi pajzsról szóló határozattal ellentétes-e az, ha a felügyeleti hatóságok gyakorolják az általános szerződési feltételeken alapuló adattovábbítás felfüggesztésére irányuló hatáskörüket.

74 A folyamatban lévő T-738/16. sz. La Quadrature du Net és társai kontra Bizottság ügy (HL 2017. C 6., 39. o.).

75 Egyebekben megjegyem, hogy írásbeli észrevételeiben a DPC nem foglalt állást az adatvédelmi pajzsról szóló határozatnak az elé terjesztett panasz elbírálására gyakorolt hatásáról.

76 Lásd e tekintetben: Schrems ítélet (78. pont).

184. E tekintetben először is nem kizárt, hogy a DPC-nek fel kell függesztenie a szóban forgó adattovábbítást, az Egyesült Államok által az érintettek alapvető jogait érintő, az amerikai hírszerző szolgálatok tevékenységéből következő jogsértésekkel szemben biztosított védelem állítólagos meg nem feleléséből következő indokoktól eltérő okokból. A kérdést előterjesztő bíróság így kiemelte, hogy M. Schrems a DPC-hez benyújtott panaszában előadja, hogy a Facebook Ireland által ezen adattovábbítás alátámasztása céljából hivatkozott szerződéses feltételek nem tükrözik hűen a 2010/87 határozat mellékletében rögzített feltételeket. M. Schrems ezenkívül azt állítja, hogy az említett adattovábbítás nem e határozat hatálya alá tartozik, hanem más ÁSZF-határozatok hatálya alá.[77]

185. Másodszor, a DPC és a kérdést előterjesztő bíróság hangsúlyozta, hogy a Facebook Ireland az M. Schrems panaszában hivatkozott adattovábbítás alátámasztására nem hivatkozott az adatvédelmi pajzsról szóló határozatra,[78] amit a tárgyalás során e társaság is megerősített. Noha a Facebook Inc. 2016. szeptember 30. óta öntanúsítással rendelkezik az adatvédelmi pajzs elveihez való csatlakozásról,[79] a Facebook Ireland azt állítja, hogy e csatlakozás csak egyes adatkategóriák, mégpedig a Facebook Inc. üzleti partnereire vonatkozó adatok továbbítását érinti. Álláspontom szerint helytelen lenne, ha a Bíróság előrevetítené azokat a kérdéseket, amelyek e tárgyban felmerülhetnek, megvizsgálva azt, hogy azt feltételezve, hogy a Facebook Ireland a szóban forgó adattovábbítás alátámasztása érdekében nem hivatkozhat a 2010/87 határozatra, ez az adattovábbítás mégis az adatvédelmi pajzsról szóló határozat hatálya alá tartozik-e, noha a Facebook Ireland ezt az érvet nem hozta fel sem a kérdést előterjesztő bíróság, sem a DPC előtt.

186. Mindezek alapján megállapítom, hogy az előzetes döntéshozatalra előterjesztett második, harmadik, negyedik, ötödik kérdés, illetve kilencedik és tizedik kérdés megválaszolásának, valamint az adatvédelmi pajzsról szóló határozat érvényessége vizsgálatának nincs helye.

G. Az adatvédelmi pajzsról szóló határozat joghatásaival és érvényességével kapcsolatos kiegészítő észrevételek

187. Noha a fenti elemzés alapján azt javaslom a Bíróságnak, hogy elsődlegesen ne határozzon az adatvédelmi pajzsról szóló határozatnak az M. Schrems által a DPC-hez benyújtotthoz hasonló panasz elbírálására gyakorolt hatásáról, valamint e határozat érvényességről, álláspontom szerint másodlagosan és fenntartásokkal érdemes néhány nem kimerítő észrevételt tenni e tárgyat illetően.

1. Az adatvédelmi pajzsról szóló határozat hatásáról egy szerződéses garanciákon alapuló adattovábbítás jogszerűségével kapcsolatos panasz felügyeleti hatóság általi elbírálása során

188. Az előzetes döntéshozatalra előterjesztett kilencedik kérdés azt veti fel, hogy az adatvédelmi pajzsról szóló határozatban a továbbított adatokhoz való hozzáférést és az adatok amerikai hatóságok által nemzetbiztonsági célokra történő felhasználását illető korlátozásokra, valamint az érintettek jogvédelmére tekintettel az Egyesült Államokban biztosított védelmi szint megfelelő jellegével kapcsolatban tett állítás akadályát jelenti-e annak, hogy a felügyeleti hatóság felfüggesszen egy ezen országba irányuló, általános szerződési feltételeken alapuló adattovábbítást.

77 M. Schrems ezen állítás alátámasztására előadja, hogy a Facebook Inc.-et nem pusztán adatfeldolgozónak kell tekinteni, hanem a GDPR 4. cikke (7) bekezdésének értelmében vett „adatkezelőnek” is, a Facebook közösségi háló felhasználói személyes adatainak kezelése tekintetében. Lásd e tekintetben: 2018. június 5-i Wirtschaftsakademie Schleswig-Holstein ítélet (C-210/16, EU:C:2018:388, 30. pont).

78 Lásd a High Court (felsőbíróság) 2017. október 3-i ítéletét (66. pont).

79 Lásd az adatvédelmi pajzs honlapját (https://www.privacyshield.gov/participant_search).

189. E problémakört álláspontom szerint a Schrems ítélet 51. és 52. pontja alapján kell felfogni, amelyből kitűnik, hogy a megfelelőségi határozat addig kötelezi a felügyeleti hatóságokat, amíg nem nyilvánítják azt érvénytelenné. Az a felügyeleti hatóság, amelyhez egy olyan személy nyújtott be panaszt, akinek adatait megfelelőségi határozattal érintett harmadik országba továbbították, tehát nem függesztheti fel az adattovábbítást azzal az indokkal, hogy az említett országban a védelmi szint nem megfelelő, anélkül hogy a Bíróság ne nyilvánította volna előzetesen érvénytelenné az említett határozatot.[80]

190. A kérdést előterjesztő bíróság lényegében azt kívánja megtudni, hogy az adatvédelmi pajzsról szóló határozathoz vagy azt megelőzően a „biztonságos kikötő" határozathoz hasonló, a vállalkozások határozatban szereplő elvekhez való önkéntes csatlakozásán alapuló megfelelőségi határozat esetében e következtetés csak abban esetben érvényes-e, ha a szóban forgó harmadik országba irányuló adattovábbítás az említett határozat hatálya alá tartozik, vagy akkor is, ha az eltérő jogalapon alapul.

191. M. Schrems, a német, a holland, a lengyel és a portugál kormány, valamint a Bizottság szerint az adatvédelmi pajzsról szóló határozatban rögzített megfelelőségi megállapítás nem fosztja meg a felügyeleti hatóságokat azon hatáskörüktől, hogy felfüggesszék vagy megtiltsák az Egyesült Államokba irányuló, általános szerződési feltételeken alapuló adattovábbítást. Amennyiben az Egyesült Államok felé irányuló adattovábbítás nem az adatvédelmi pajzsról szóló határozaton alapul, a felügyeleti hatóságokat e határozat formailag nem kötelezi a GDPR 58. cikkének (2) bekezdésében rájuk ruházott hatáskörök gyakorlása során. Másként fogalmazva, e hatóságok eltérhetnek a Bizottságnak az amerikai hatóságok érintett személyek alapvető jogainak gyakorlásába történő beavatkozásával szembeni védelem szintjének megfelelőségére vonatkozó megállapításaitól. A holland kormány és a Bizottság kiemeli, hogy a felügyeleti hatóságoknak ugyanakkor figyelembe kell venniük ezeket, amikor e hatásköröket gyakorolják. A német kormány véleménye szerint e hatóságok csak a Bizottság által tett megállapítások a releváns elemekre kiterjedő elemzést magában foglaló, érdemi vizsgálatának eredményeként juthatnak ellentétes értékelésre.

192. Ezzel szemben a Facebook Ireland és az Egyesült Királyság kormánya lényegében azt adja elő, hogy a megfelelőségi határozat kötelező hatálya a jogbiztonság és az uniós jog egységes alkalmazása követelményeinek fényében azt jelenti, hogy a felügyeleti hatóságok nem jogosultak az említett határozatban szereplő megállapítások megkérdőjelezésére, még az e határozattól eltérő jogalapon a szóban forgó harmadik országba irányuló adatáramlások felfüggesztésére irányuló panasz elbírálásával összefüggésben sem.

193. E két megközelítés közül az elsővel értek egyet. Mivel az adatvédelmi pajzsról szóló határozat hatálya az e határozat alapján öntanúsítással rendelkező vállalkozások részére végzett adattovábbításokra korlátozódik, az említett határozat formálisan nem kötelezheti a felügyeleti hatóságokat azon adattovábbítások tekintetében, amelyek nem tartoznak e hatály alá. Az adatvédelmi pajzsról szóló határozat ehhez hasonlóan a jogbiztonságot csak azon adatátadók vonatkozásában kívánja garantálni, amelyek az általa rögzített keretben végeznek adattovábbítást. Álláspontom szerint a felügyeleti hatóságok GDPR 52. cikkében elismert függetlenségével is ellentétes lenne az, ha még a határozat hatályán kívül is kötelezné őket a Bizottság által a megfelelőségi határozatban tett megállapítások.

194. Természetesen az adatvédelmi pajzsról szóló határozatban szereplő, az Egyesült Államokban a hírszerző szolgálatok tevékenységével kapcsolatos beavatkozásokkal szemben biztosított védelmi szint megfelelőségére vonatkozó megállapítások képezik a kiindulópontját annak az elemzésnek, amely révén a felügyeleti hatóság esetről esetre értékeli, hogy egy általános szerződési feltételeken alapuló

80 Lásd ebben az értelemben: Schrems ítélet (59. pont).

adattovábbítást fel kell-e függeszteni az ilyen beavatkozások miatt. Ha ugyanakkor alapos vizsgálatot követően úgy ítéli meg, hogy nem tud egyetérteni e megállapításokkal az elé terjesztett adattovábbítást illetően, a felügyeleti hatóság álláspontom szerint megőrzi lehetőségét a GDPR 58. cikke (2) bekezdésének f) és j) pontjával ráruházott hatáskörök gyakorlására.

195. Ezt követően, amennyiben a Bíróság az itt megvizsgált kérdésre az általam javasolttal ellentétes választ kívánna adni, akkor meg kellene vizsgálni, hogy e hatásköröket nem kell-e mégis visszaállítani az adatvédelmi pajzsról szóló határozat érvénytelensége miatt.

2. Az adatvédelmi pajzsról szóló határozat érvényességéről

196. Az alábbi megfontolások bizonyos kérdéseket vetnek fel az Egyesült Államok által az amerikai hírszerzési hatóságok által az elektronikus kommunikáció megfigyelésével kapcsolatban folytatott tevékenységekkel összefüggésben biztosított védelmi szint GDPR 45. cikke (1) bekezdésének értelmében vett megfelelő jellege kapcsán, az adatvédelmi pajzsról szóló határozatban található értékelések megalapozottságát illetően. Ezek az észrevételek nem arra irányulnak, hogy végleges vagy kimerítő álláspontot ismertessek e határozat érvényességét illetően. Pusztán olyan reflexiókat tartalmaznak, amelyek hasznosak lehetnek a Bíróság számára, amennyiben javaslatommal ellentétesen kívánna dönteni e kérdést illetően.

197. E vonatkozásban az adatvédelmi pajzsról szóló határozat (64) preambulumbekezdéséből és II. melléklete I. szakaszának 5. pontjából kitűnik, hogy az e határozatban rögzített elvekhez való csatlakozást korlátozhatják többek között a nemzetbiztonsággal, a közérdekkel és a törvény tiszteletben tartásával kapcsolatos követelmények, valamint az amerikai jogból fakadó kötelezettségek.

198. A Bizottság ezért értékelte az Egyesült Államok jogában a továbbított adatokhoz való amerikai hatóságok általi, különösen nemzetbiztonsági célú hozzáférést és azok felhasználását érintően biztosított garanciákat.[81] Az amerikai kormány bizonyos kötelezettségvállalásokat tett a Bizottság felé, amelyek egyrészt a továbbított adatokhoz való amerikai hatóságok általi, különösen nemzetbiztonsági célú hozzáférést és azok felhasználását érintik, másrészt pedig az érintett számára biztosított jogvédelmet.[82]

199. A Bíróság előtt M. Schrems az adatvédelmi pajzsról szóló határozat érvénytelenségére hivatkozik, azzal az indokkal, hogy az ily módon ismertetett garanciák nem elegendőek azon személyek alapvető jogait illetően a megfelelő védelmi szint biztosítására, akiknek adatait az Egyesült Államokban továbbították. A DPC, az EPIC, az osztrák, a lengyel és a portugál kormány, anélkül hogy közvetlenül

81 Lásd az adatvédelmi pajzsról szóló határozat (65) preambulumbekezdését.

82 Lásd az adatvédelmi pajzsról szóló határozat III–VII. mellékletét.

megkérdőjelezné e határozat érvényességét, vitatja a Bizottság által abban az amerikai hírszerző szolgálatok tevékenységéből következő beavatkozásokkal szembeni védelem szintjének megfelelőségére vonatkozóan tett megállapításokat. E kétségek a Parlament,[83] az EDPB[84] és az európai adatvédelmi biztos[85] által kifejezett aggodalmakat tükrözik.

200. Az adatvédelmi pajzsról szóló határozatban szereplő megfelelőségi megállapítás értékelését megelőzően pontosítani kell azt a módszert, amelyet e vizsgálat során követni kell.

a) A megfelelőségi határozat érvényességével kapcsolatos vizsgálat tartalmára vonatkozó pontosítások

1) A védelmi szint „lényegi azonosságának” értékelését lehetővé tévő összehasonlítás feltételei

201. A GDPR 45. cikke (3) bekezdésének, valamint a Bíróság ítélkezési gyakorlatának[86] megfelelően a Bizottság csak akkor állapíthatja meg, hogy egy harmadik ország megfelelő védelmi szintet biztosít, ha kellően megindokolt módon megállapította, hogy az érintett alapvető jogainak védelmi szintje az említett országban „lényegében azonos” az Unióban ezen, a Charta fényében értelmezett rendelet által megkövetelt szinttel.

202. Ily módon a harmadik országban biztosított védelmi szint megfelelőségének vizsgálata szükségképpen egyfelől az e harmadik országban érvényesülő szabályok és gyakorlatok, másfelől pedig az Unióban érvényes védelmi standardok összehasonlításával jár. Második kérdésével az előterjesztő bíróság arra kéri a Bíróságot, hogy pontosítsa ezen összehasonlítás feltételeit.[87]

203. Konkrétabban e bíróság azt kívánja megtudni, hogy az EUSZ 4. cikk (2) bekezdése és a GDPR 2. cikkének (2) bekezdése által elismert, a nemzetbiztonság területén a tagállamoknak fenntartott hatáskör azt jelenti-e, hogy az uniós jogrend nem tartalmaz olyan védelmi standardokat, amelyekkel a megfelelőség értékelése céljából össze kell hasonlítani a valamely harmadik országban a hatóságok részéről a továbbított adatok nemzetbiztonsági célú kezelését övező garanciákat. Igenlő válasz esetén a bíróság azt kívánja megtudni, hogy miként kell meghatározni a releváns viszonyítási alapot.

83 Az EU–USA adatvédelmi pajzs által nyújtott védelem megfelelőségéről szóló, 2017. április 6-i európai parlamenti állásfoglalás, P8_TA(2017)0131, valamint az EU–USA adatvédelmi pajzs által nyújtott védelem megfelelőségéről szóló, 2018. július 5-i európai parlamenti állásfoglalás, P8_TA(2018)0315.

84 Lásd: a 29. cikk alapján létrehozott adatvédelmi munkacsoport (a továbbiakban: 29. csoport), Opinion 1/2016 on the EU-U. S. Privacy Shield draft adequacy decision, 2016. április 13., WP 238; 29. csoport, EU-US Privacy Shield – First Annual Joint Review, 2017. november 28., WP 255, valamint EDPB, EU-US Privacy Shield – Second Annual Joint Review, 2019. január 22. A 29. csoportot a 95/46 irányelv 29. cikkének (1) bekezdése alapján hozták létre, amely előírta, hogy a csoport tanácsadói státuszban működik és függetlenül jár el. E cikk (2) bekezdése szerint e csoport az egyes nemzeti felügyelő hatóságok képviselőjéből, a közösségi intézmények és szervek nevében létrehozott egyes hatóságok képviselőjéből, továbbá a Bizottság egy képviselőjéből áll. A GDPR hatálybalépése óta a 29. csoportot az EDPB váltotta fel (lásd e rendelet 94. cikkének (2) bekezdését).

85 Lásd az európai adatvédelmi biztos EU–USA adatvédelmi pajzs megfelelőségéről szóló határozattervezetről szóló, 2016. május 30-i 4/2016. sz. véleményét. Az európai adatvédelmi biztos intézményét a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2001. december 18-i 45/2001/EK európai parlamenti és tanácsi rendelet (HL 2001. L 8., 1. o.; magyar nyelvű különkiadás 13. fejezet, 26. kötet, 102. o.) 1. cikkének (2) bekezdése hozta létre. A biztos e rendelet rendelkezéseinek alkalmazását ellenőrzi.

86 Lásd a jelen indítvány 112. pontját.

87 Emlékeztetek arra, hogy a harmadik ország által biztosított védelmi szint lényegi egyenértékűségét az Unió által megkövetelthez képest akkor is értékelni kell, amikor a 2010/87 határozatban előírt általános szerződési feltételeken alapuló konkrét adattovábbítással összefüggésben az adatkezelő, illetve ennek hiányában az illetékes felügyeleti hatóság megvizsgálja, hogy a célországnak számító harmadik ország hatóságai olyan követelményeket támasztanak-e az adatátvevővel szemben, amelyek túllépnek a demokratikus társadalomban szükséges rendelkezéseken korlátain (lásd a 2010/87 határozat mellékletében található 5. általános szerződési feltételt, valamint az arra vonatkozó lábjegyzetet). Lásd a jelen indítvány 115., 134. és 135. pontját.

204. E vonatkozásban szem előtt kell tartani, hogy az uniós jog által a személyes adatok nemzetközi továbbítása tekintetében meghatározott, az érintettek jogait érintő védelmi szint folytonosságának biztosítását megkövetelő korlátozások indoka az, hogy elkerüljék az Unión belül alkalmazandó standardok kijátszásának kockázatát.[88] Amint azt lényegében a Facebook Ireland kifejti, e célra tekintettel egyáltalán nem lenne igazolt, ha a harmadik országtól olyan követelmények tiszteletben tartását várnák el, amelyek nem felelnek meg a tagállamokat terhelő kötelezettségeknek.

205. Az 51. cikkének (1) bekezdése szerint a Charta a tagállamokra csak akkor alkalmazandó, amennyiben azok az Unió jogát hajtják végre. Következésképpen egy megfelelőségi határozat érvényessége, figyelemmel az érintettek célországnak számító harmadik ország szabályozásából következő alapvető jogainak gyakorlását érintő korlátozásokra, csak akkor függ e korlátozások és a tagállamok részéről a Charta rendelkezései által engedélyezett korlátozások összehasonlításától, *ha a tagállam hasonló szabályozása az uniós jog hatálya alá tartozna*.

206. Ugyanakkor a célországnak számító harmadik országban biztosított védelmi szint megfelelőségét nem lehet az érintettek alapvető jogainak gyakorlását érintő, többek között a nemzetbiztonság területén érvényesített olyan állami intézkedésekből fakadó esetleges beavatkozások figyelmen kívül hagyásával értékelni, amelyek, ha azokat valamely tagállam fogadná el őket, az uniós jog hatályán kívül esnének. Ezen értékelés céljából a GDPR 45. cikke (2) bekezdésének a) pontja az e harmadik országban hatályos nemzetbiztonsági szabályozások korlátozás nélküli figyelembevételét követeli meg.

207. Az állami intézkedések megfelelőségének e védelmi intézkedésekre tekintettel történő értékelése álláspontom szerint azt vonja maga után, hogy az ezen intézkedésekhez kapcsolódó garanciákat össze kell hasonlítani az Unión belül a tagállamok joga által előírt védelmi szinttel, beleértve az általuk az EJEE alapján vállalt kötelezettségeket is. Mivel a tagállamok EJEE-hez való csatlakozása arra kötelezi őket, hogy belső jogukat hozzák összhangba ezen egyezmény rendelkezéseivel, és az ily módon, amint azt lényegében a Facebook Ireland, a német és a cseh kormány, valamint a Bizottság hangsúlyozta, közös nevezőt képez a tagállamok vonatkozásában, e rendelkezéseket tekintem az említett értékelés céljából a releváns összehasonlítási alapnak.

208. A jelen esetben, amint azt fent kifejtettem,[89] az Egyesült Államok nemzetbiztonságával kapcsolatos követelmények elsőbbséget élveznek az adatvédelmi pajzsról szóló határozat alapján az öntanúsítással rendelkező vállalkozásokat terhelő kötelezettségekkel szemben. Így tehát e határozat érvényessége attól a kérdéstől függ, hogy e követelményekhez olyan garanciák kapcsolódnak-e, amelyek lényegében azonos védelmi szintet biztosítanak, mint amelyet az Unióban kell biztosítani.

209. Az e kérdésre adandó válaszhoz előzetesen azonosítani kell azokat a standardokat – vagyis a Chartán és az EJEE-n alapuló standardokat – amelyeknek az Unión belül a Bizottság által az adatvédelmi pajzsról szóló határozatban vizsgáltakhoz hasonló, az elektronikus kommunikáció megfigyelésével kapcsolatos szabályozásoknak meg kell felelniük. Az alkalmazandó standardok azonosítása attól a kérdéstől függ, hogy a FISA 702. cikkéhez és az EO 12333-hoz hasonló szabályozások, ha valamely tagállamtól származnának, a GDPR hatályát érintő, e rendelet 2. cikkének az EUSZ 4. cikk (2) bekezdése fényében értelmezett (2) bekezdésén alapuló korlátozás alá esnének-e.

88 Lásd a jelen indítvány 117. pontját.

89 Lásd a jelen indítvány 197. pontját.

210. Ezzel kapcsolatban az EUSZ 4. cikk (2) bekezdéséből, valamint az állandó ítélkezési gyakorlatból kitűnik, hogy az uniós jog és különösen a személyes adatok védelmére vonatkozó másodlagos jogi aktusok nem alkalmazandók a nemzetbiztonság védelmével kapcsolatos tevékenységekre, mivel azok az állam vagy az állami hatóságok sajátos tevékenységei, és nem tartoznak a magánszemélyek tevékenységei közé. [90]

211. Ez az elv *egyrészt* azt jelenti, hogy a nemzetbiztonság védelmével kapcsolatos szabályozás nem tartozik az uniós jog hatálya alá, amennyiben kizárólag állami tevékenységeket szabályoz, a magánszemélyek tevékenységei pedig teljesen kívül esnek azon. Következésképpen e jog álláspontom szerint nem alkalmazandó a személyes adatok gyűjtésével és felhasználásával kapcsolatos, az állam által a nemzetbiztonság védelme céljából közvetlenül végrehajtott, a magángazdasági szereplőkre sajátos kötelezettséggel nem járó nemzeti intézkedésekre. Közelebbről, amint azt a Bizottság a tárgyalás során kifejtette, a tagállam által hozott, az EO 12333-hoz hasonlóan a biztonsági szolgálatok számára az állam területe felé továbbított adatokhoz közvetlen hozzáférést engedő intézkedések nem tartoznak az uniós jog hatálya alá. [91]

212. Egyébként jóval összetettebb *másrészt* az a kérdés, hogy azok a nemzeti rendelkezések, amelyek a FISA 702. cikkéhez hasonlóan arra kötelezik a nemzeti elektronikus hírközlési szolgáltatókat, hogy a nemzetbiztonság területén nyújtsanak támogatást az illetékes hatóságok számára, annak érdekében, hogy lehetővé tegyék hozzáférésüket bizonyos személyes adatokhoz, szintén kívül esnek-e az uniós jog hatályán.

213. Míg a PNR ítélet az e kérdésre adandó igenlő válasz mellett szól, addig a Tele2 Sverige ítéletben és a Ministerio Fiscal ítéletben követett okfejtés nemleges választ indokolhatna.

214. A PNR ítéletben a Bíróság megsemmisítette azt a határozatot, amellyel a Bizottság megállapította, hogy a légi utasok utasnyilvántartási adatállományában tárolt, az amerikai vám- és határvédelmi hatóság részére továbbított személyes adatok (Passenger Name Records, PNR) védelme megfelelő szintű. [92] A Bíróság megállapította, hogy az e határozat tárgyát képező adatkezelés – vagyis a PNR-adatok légitársaságok által továbbítása a szóban forgó hatóság felé – *tárgyára tekintettel* a 95/46 irányelv 3. cikkének (2) bekezdése alapján ki van zárva az irányelv hatálya alól. A Bíróság szerint ez az adatkezelés nem szolgáltatás nyújtásához, hanem a közbiztonság fenntartása és a bűnüldözés érdekében

90 Lásd többek között: 2003. november 6-i Lindqvist ítélet (C-101/01, EU:C:2003:596, 43. és 44. pont); PNR ítélet (58. pont); 2008. december 16-i Satakunnan Markkinapörssi és Satamedia ítélet (C-73/07, EU:C:2008:727, 41. pont); 2016. december 21-i Tele2 Sverige és Watson és társai ítélet (C-203/15 és C-698/15, EU:C:2016:970, a továbbiakban: Tele2 Sverige ítélet, 69. pont); 2018. október 2-i Ministerio Fiscal ítélet (C-207/16, EU:C:2018:788, a továbbiakban: Ministerio Fiscal ítélet, 32. pont).

91 E kérdést illetően az egyértelműség kedvéért hangsúlyozom, hogy az adatvédelmi pajzsról szóló határozatban a Bizottság nem tudta meghatározni, hogy az Egyesült Államok ténylegesen lehallgatja-e a transzatlanti kábeleken áthaladó közléseket, mivel az amerikai hatóságok nem erősítették meg és nem is cáfolták e felvetést (lásd e határozat (75) preambulumbekezdését, valamint Robert Litt 2016. február 22-i levelét, amely a határozat VI. melléklete I. pontjának a) alpontjában található). Ugyanakkor mivel az Egyesült Államok kormánya nem tagadta, hogy az EO 12333 alapján gyűjti az állam területe felé továbbított adatokat, álláspontom szerint a Bizottságnak a megfelelőség megállapítása előtt biztosítékokat kellett szereznie e kormánytól, amelyek szerint erre az adatgyűjtésre, amennyiben arra sor kerülne, megfelelő garanciák vonatkoznának a visszaélés kockázatával szemben. A Bizottság az említett határozat (68)–(77) preambulumbekezdésében ebből a szempontból vizsgálta meg azokat a korlátozásokat és garanciákat, amelyeket a PPD 28 alapján ilyen helyzetben alkalmazni kell.

92 Az Egyesült Államok Vámügyi és Határvédelmi Irodája rendelkezésére bocsátott, a légi utasok utasnyilvántartási adatállományában tárolt személyes adatok megfelelő védelméről szóló, 2004. május 14-i 2004/535/EK bizottsági határozatról (HL 2011. L 235., 11. o.) volt szó.

volt szükséges. Mivel a szóban forgó adattovábbítás háttere közhatalmi jellegű és közbiztonsági célú volt, az nem tartozott az említett irányelv hatálya alá, annak ellenére, hogy a PNR-adatokat eredetileg magángazdasági szereplők gyűjtötték az említett irányelv hatálya alá tartozó kereskedelmi tevékenység keretében, valamint az adattovábbítást az utóbbiak szervezték meg.[93]

215. Az ezt követő Tele2 Sverige ítéletben[94] a Bíróság azt mondta ki, hogy a 2002/58/EK irányelv[95] 15. cikkének (1) bekezdésén alapuló, mind a forgalmi és helymeghatározó adatok hírközlési szolgáltatók általi tárolását, mind pedig a hatóságok tárolt adatokhoz való, az érintett rendelkezésekben meghatározott – a bűnüldözésre és a nemzetbiztonság védelmére is kiterjedő – célú hozzáférését szabályozó nemzeti rendelkezések az említett irányelv, és ebből következően a Charta hatálya alá tartoznak. A Bíróság szerint sem az adattárolásra vonatkozó rendelkezések, sem a tárolt adatokhoz való hozzáférésre vonatkozó rendelkezések nem tartoznak az irányelv hatálya alóli, az irányelv 1. cikkének (3) bekezdésében előírt kivétel alá, amely többek között a bűnüldözéssel és a nemzetbiztonság védelmével kapcsolatos állami tevékenységekre utal.[96] A Bíróság a Ministerio Fiscal ítéletben[97] megerősítette ezt az ítélkezési gyakorlatot.

216. A FISA 702. cikke ugyanakkor eltér az ilyen szabályozástól, mivel e rendelkezés nem telepít semmilyen, az adatok tárolására, illetve a hírszerzési hatóságoktól származó, az adatokhoz való hozzáférés iránti megkeresés hiányában más adatkezelés végzésére irányuló kötelezettséget az elektronikus hírközlési szolgáltatókra.

217. Ezért felmerül a kérdés, hogy a GDPR és ebből következően a Charta hatálya alá tartoznak-e az olyan nemzeti intézkedések, amelyek *bármely tárolási kötelezettségtől függetlenül* arra kötelezik e szolgáltatókat, hogy nemzetbiztonsági célból bocsássanak adatokat a hatóságok rendelkezésére.[98]

218. Az *első megközelítés* az lehetne, hogy a lehető leginkább összehangoljuk az ítélkezési gyakorlat fent hivatkozott két irányvonalát, oly módon értelmezve a Bíróság által a Tele2 Sverige ítéletben és a Ministerio Fiscal ítéletben rögzített, az uniós jog azon intézkedésekre való alkalmazhatóságára vonatkozó megállapítást, amelyek a hatóságok többek között nemzetbiztonsági célú adathozzáférését

93 PNR ítélet (56–58. pont). Egyébként a 2009. február 10-i Írország kontra Parlament és Tanács ítéletben (C-301/06, EU:C:2009:68, 90. és 91. pont) a Bíróság megállapította, hogy a PNR-ítéletben kifejtett megfontolások nem ültethetők át a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról szóló, 2006. március 15-i 2006/24/EK európai parlamenti és tanácsi irányelvben (HL 2006. L 105., 54. o.; helyesbítés: HL 2009. L 50., 52. o.) hivatkozott adatkezelésekre. A Bíróság e megállapítást azzal indokolta, hogy a 2006/24 irányelv a PNR ítéletben szereplő határozattól eltérően kizárólag a belső piacon működő szolgáltatásnyújtók tevékenységére vonatkozik, és nem tartalmaz szabályozást a közhatalmi szervek bűnüldöző tevékenységeit illetően. Ezen okfejtéssel a Bíróság láthatóan azt állította, hogy *a contrario* a PNR ítéletben szereplő következtetés átültethető a tárolt adatokhoz való, ezen hatóság általi hozzáféréssel, illetve azok felhasználásával kapcsolatos rendelkezésekre.

94 Tele2 Sverige ítélet (67–81. pont).

95 Az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv (egyetemes szolgáltatási irányelv) (HL 2002. L 201., 37. o.; magyar nyelvű különkiadás 13. fejezet, 29. kötet, 514. o.).

96 Mivel a 2002/58 irányelv az azóta a tartalmát nagymértékben átvevő GDPR által hatályon kívül helyezett 95/46 irányelv követelményeit konkretizálja, a 2002/58 irányelv 1. cikke (3) bekezdésének értelmezésére vonatkozó ítélkezési gyakorlat analógia útján alkalmazandónak tűnik a GDPR 2. cikke (2) bekezdésének értelmezése kapcsán. Lásd ebben az értelemben: Tele2 Sverige ítélet (69. pont), valamint Ministerio Fiscal ítélet (32. pont).

97 Ministerio Fiscal ítélet (34., 35. és 37. pont).

98 Ugyanezen kérdés a Bíróság előtt folyamatban lévő három másik előzetes döntéshozatali iránti kérelem tárgyát képezi. Lásd: C-623/17, Privacy International ügy (HL 2018. C 22., 29. o.); C-511/18 és C-512/18, La Quadrature du Net és társai, valamint French Data Network és társai egyesített ügyek (HL 2018. C 392., 7. o.).

szabályozzák,[99] hogy azok azon esetekre korlátozódnak, amelyekben az adatokat a 2002/58 irányelv 15. cikkének (1) bekezdése alapján bevezetett *jogszabályi kötelezettség alapján* tárolják. E megállapítás ellenben nem alkalmazandó a PNR ítélet eltérő ténybeli hátterére, amely a légitársaságok által kereskedelmi célból tárolt adatok egy illetékes amerikai belbiztonsági hatóság részére történő továbbítására vonatkozott, azok saját kezdeményezésére.

219. A Bizottság által támogatott és általam is meggyőzőbbnek ítélt *második megközelítés* szerint a Tele2 Sverige ítéletben és a Ministerio Fiscal ítéletben követett okfejtés igazolja az uniós jog alkalmazhatóságát az elektronikus hírközlési szolgáltatók számára azt előíró nemzeti szabályokra, hogy nyújtsanak segítséget a nemzetbiztonságért felelős hatóságok számára annak érdekében, hogy azok hozzáférhessenek bizonyos adatokhoz, *anélkül hogy releváns lenne, hogy e szabályok az adatok előzetes tárolására irányuló kötelezettséghez kapcsolódnak-e, vagy sem*.

220. Ezen okfejtés fókuszában ugyanis nem a szóban forgó rendelkezések célja áll, mint a PNR ítélet esetében, hanem az, hogy e rendelkezések a szolgáltatók tevékenységét szabályozzák, adatkezelést írva elő számukra. E tevékenységek nem minősültek állami tevékenységnek a 2002/58 irányelv 1. cikkének (3) bekezdésében és a 95/46 irányelv 3. cikkének (2) bekezdésében – amelynek tartalmát a GDPR 2. cikkének (2) bekezdése lényegében átveszi – hivatkozott területeteken.

221. Ily módon a Tele2 Sverige ítéletben a Bíróság megjegyezte, hogy „[a] szolgáltatók által tárolt adatokhoz [való hozzáférés] a személyes adatok *ez utóbbiak általi* kezelésére vonatkozik, ami ezen irányelv hatálya alá tartozik”.[100] A Ministerio Fiscal ítéletben a Bíróság ugyanígy kimondta, hogy az elektronikus hírközlési szolgáltatókat arra kötelező jogszabályi intézkedések, hogy a hatáskörrel rendelkező hatóságoknak biztosítsanak hozzáférést a tárolt adatokhoz, „szükségképpen magában foglalja az említett adatok *e szolgáltatók* általi kezelését”.[101]

222. Márpedig az adatkezelő részéről az adatoknak a hatóság rendelkezésére bocsátása megfelel a GDPR 4. cikkének (2) bekezdésében rögzített „adatkezelés” fogalmának.[102] Ugyanez vonatkozik az adatok keresési feltételek révén történő előzetes szűrésére, annak érdekében, hogy elszigeteljék azokat, amelyekhez a hatóságok hozzáférést igényeltek.[103]

223. Mindezek alapján megállapítom, hogy a Bíróság által a Tele2 Sverige ítéletben és a Ministerio Fiscal ítéletben követett okfejtés nyomán a GDPR, és ebből következően a Charta alkalmazandó az olyan nemzeti szabályozásra, amely arra kötelezi az elektronikus hírközlési szolgáltatót, hogy nyújtson segítséget a nemzetbiztonságért felelős hatóságok számára, adatokat bocsátva rendelkezésükre, adott esetben szűrést követően, még az ezen adatok tárolására vonatkozó jogszabályi kötelezettség hiányában is.

99 A Tele2 Sverige ítéletben, noha a Bíróság a szóban forgó tárolási és hozzáférési intézkedésekből következő beavatkozások igazolásának vizsgálatára koncentrált, a bűncselekmények elleni küzdelem céljára figyelemmel, az általa levont következtetés megfelelően alkalmazandó akkor is, ha az ilyen intézkedések a nemzetbiztonság védelmére irányuló célt követnek. A 2002/58 irányelv 15. cikkének (1) bekezdése ugyanis az ilyen intézkedések igazolására alkalmas célok között hivatkozik mind a bűncselekmények elleni küzdelemre, mind a nemzetbiztonság védelmére. Egyébként a 2002/58 irányelv 1. cikkének (3) bekezdése és a GDPR 2. cikkének (2) bekezdése kizárják az említett jogi aktusok hatálya alól az állami tevékenységeket mind a nemzetbiztonság, mind pedig a büntetőjog területén. A Tele2 Sverige ítélet alapjául szolgáló ügyben szereplő intézkedések egyébként a nemzetbiztonsággal kapcsolatos célt is követtek. Ezen ítélet 119. pontjában a Bíróság kifejezetten kitért a forgalmi és helymeghatározó adatok tárolásával és az azokhoz való hozzáféréssel kapcsolatos intézkedések igazolására a nemzetbiztonság védelmének céljára tekintettel, amennyiben az magában foglalja a terrorizmus elleni küzdelmet.

100 Tele2 Sverige ítélet (78. pont, kiemelés tőlem). Amint azt a „továbbá” kifejezés használata is mutatja, a Bíróság kizárólag a 2002/58 irányelv alkalmazhatóságára vonatkozó következtetésének alátámasztása céljából hangsúlyozta ezen ítélet 79. pontjában az ezen ítélet alapjául szolgáló ügyben a szóban forgó adatok tárolására irányuló kötelezettség és a nemzeti hatóságok tárolt adatokhoz való hozzáférésére vonatkozó rendelkezések közötti szerves kapcsolatot.

101 Ministerio Fiscal ítélet (37. pont, kiemelés tőlem).

102 Lásd ebben az értelemben: Ministerio Fiscal ítélet (38. pont).

103 Lásd ebben az értelemben: 2014. május 13-i Google Spain és Google ítélet (C-131/12, EU:C:2014:317, 28. pont).

224. Ezenfelül láthatóan ez az értelmezés következik, legalábbis hallgatólagosan, a Schrems ítéletből. Amint azt a DPC, az osztrák és a lengyel kormány, valamint a Bizottság hangsúlyozta, a Bíróság a „biztonságos kikötő” határozat érvényességének vizsgálata során kimondta, hogy a megfelelőségi határozat által érintett harmadik ország jogának a hatóságok érintettek alapvető jogaiba való nemzetbiztonsági célú beavatkozásaival szemben lényegében azonos garanciákat kell nyújtania, mint amelyek a Charta 7., 8. és 47. cikkéből következnek.[104]

225. Ebből konkrétabban az következik, hogy nem tartozik a GDPR 2. cikke (2) bekezdésének hatálya alá az elektronikus hírközlési szolgáltatók számára azt előíró nemzeti intézkedés, hogy teljesítsék a nemzetbiztonságért felelős illetékes hatóságok e szolgáltatók által bármely jogi kötelezettségtől függetlenül üzleti tevékenységük során tárolt adatokhoz való hozzáférés iránti megkeresését, a kért adatokat előzetesen kiválasztási tényezők alkalmazása révén azonosítva (mint a PRISM-program keretében). Ugyanez vonatkozik az olyan nemzeti intézkedésre, amely arra kötelezi a távközlési „gerinchálózatot” üzemeltető vállalkozásokat, hogy biztosítsanak hozzáférést a nemzetbiztonságért felelős hatóságok számára az általuk üzemeltetett infrastruktúrán áthaladó adatokhoz (mint az Upstream program során).

226. Ezzel szemben azt követően, hogy az adatok az állami hatóságok birtokába kerültek, e hatóságok általi későbbi nemzetbiztonsági célú tárolásukra és felhasználásukra a fenti 211. pontban kifejtettekkel azonos okokból álláspontom szerint kiterjed a GDPR 2. cikkének (2) bekezdésében előírt eltérés, így azok nem tartoznak e rendelet és ebből következően a Charta hatálya alá sem.

227. A fentiekre figyelemmel úgy vélem, hogy az adatvédelmi pajzsról szóló határozat érvényességének vizsgálata, az ott rögzített elvek azon korlátozásaira figyelemmel, amelyek az amerikai hírszerzési hatóságok tevékenységeiből fakadhatnak, kettős ellenőrzést igényel.

228. *Először* azt kell megvizsgálni, hogy az Egyesült Államok lényegében azonos védelmi szintet biztosít-e a FISA 702. cikkének alkalmazásából következő korlátozásokkal szemben, mint amely a GDPR és a Charta rendelkezéseiből következik, mivel e rendelkezés lehetővé teszi az NSA számára, hogy előírja a szolgáltatóknak a személyes adatok rendelkezésére bocsátását.

229. *Másodszor* az EJEE rendelkezései képeznek releváns viszonyítási alapot annak értékelése szempontjából, hogy az EO 12333 végrehajtása által eredményezhető korlátozások – amennyiben az lehetővé teszi a hírszerzési hatóságok számára, hogy a magángazdasági szereplő segítsége nélkül maguk gyűjtsenek személyes adatokat – megkérdőjelezik-e az Egyesült Államok által biztosított védelmi szint megfelelőségét. E rendelkezések szolgáltatják továbbá az e védelmi szint megfelelőségének értékelését lehetővé tévő összehasonlítási standardokat az e hatóságok által nemzetbiztonsági céllal megszerzett adatok tárolását és felhasználását illetően.

230. El kell ugyanakkor még dönteni azt, hogy a megfelelőségi megállapítás feltételezi-e azt, hogy az EO 12333-on alapuló adatgyűjtéshez lényegében azonos szintű védelem kapcsolódik-e, mint amelyet az Unión belül kell biztosítani, *még akkor is, ha erre az adatgyűjtésre az Egyesült Államok területén kívül kerül sor*, abban a szakaszban, amikor az adatokat az Unióból e harmadik ország felé továbbítják.

104 Schrems ítélet (91–96. pont). Az adatvédelmi pajzsról szóló határozat (90), (124) és (141) preambulumbekezdésében a Bizottság egyébként hivatkozott a Charta más rendelkezéseire, ily módon elfogadva azt az elvet, amely szerint az alapvető jogok nemzetbiztonsági célú korlátozásainak meg kell felelniük a Chartának.

2) A megfelelő védelmi szint biztosításának szükségességéről az adattovábbítás szakaszában

231. A Bíróság előtt három eltérő álláspontot képviseltek meg azzal kapcsolatban, hogy a Bizottságnak a harmadik ország biztosított védelmi szint megfelelőségének értékelése során figyelembe kell-e vennie az e harmadik ország hatóságai adatokhoz való hozzáférésével kapcsolatos nemzeti intézkedéseket az államterületen kívül azon szakaszban, amikor az adatokat az Unióból e harmadik ország területe felé továbbítják.

232. Először is, a Facebook Ireland, valamint az Egyesült Államok és az Egyesült Királyság kormánya lényegében arra hivatkozik, hogy az ilyen intézkedések fennállása semmilyen hatást nem gyakorolt a megfelelőségi megállapítással összefüggésben. Az utóbbiak e megközelítés alátámasztására arra hivatkoznak, hogy a harmadik ország nem képes valamennyi területén kívüli olyan kommunikációs csatorna ellenőrzése, amelyen keresztül az Unióból származó adatok haladnak át, így fogalmilag soha nem lehet garantálni, hogy másik harmadik ország nem gyűjti titokban az adatokat, amikor azok továbbítás alatt állnak.

233. Másodszor, a DPC, M. Schrems, az EPIC, az osztrák és a holland kormány, a Parlament és az EDPB előadja, hogy a védelmi szint folytonosságának a GDPR 44. cikkében szereplő követelménye azt jelenti, hogy e szintnek megfelelőnek kell lennie a továbbítás teljes tartama alatt, beleértve azt is, amikor az adatok a tenger alatti kábeleken haladnák át, mielőtt elérnék a célországnak számító harmadik ország területét.

234. Ezen elv elismerése mellett a Bizottság harmadszor előadja, hogy a megfelelőségi megállapítás tárgya az érintett harmadik ország által *határain belül* nyújtott védelemre korlátozódik, így az a körülmény, amely szerint a megfelelő védelmi szint nem garantált az ezen ország felé *továbbítás alatt*, nem kérdőjelezi meg a megfelelőségi határozat érvényességét. Mindazonáltal a GDPR 32. cikkének megfelelően az adatkezelőnek kell gondoskodnia a személyes adatok továbbításának lehető legnagyobb fokú biztonságáról, amikor azokat az említett harmadik ország felé továbbítják.

235. E tekintetben megjegyzem, hogy a GDPR 44. cikke szerint harmadik országba irányuló adattovábbításra akkor kerülhet sor, ha teljesülnek az e rendelet V. fejezetének rendelkezéseiben rögzített feltételek, amennyiben „továbbításukat követően” az adatokat esetlegesen adatkezelésnek vethetik alá. E megfogalmazást vagy úgy lehetne érteni, amint azt az Egyesült Államok kormánya állította a Bíróság kérdéseire adott írásbeli válaszában, hogy e feltételeket *azt követően* kell tiszteletben tartani, *hogy az adatok rendeltetési helyükre érkeztek*, vagy pedig úgy, hogy azok *azt követően* kötelezőek, *hogy megkezdődött az adattovábbítás* (az adattovábbítási szakaszt is beleértve).

236. Mivel a GDPR 44. cikkének szövegezése nem egyértelmű, a teleologikus értelmezés alapján a második értelmezéssel értek egyet, és ebből következően a fent említett második megközelítéshez csatlakozom. Ha ugyanis úgy tekintenénk, hogy a védelmi szint folytonosságának e rendelkezésben előírt követelménye csak a célországnak számító harmadik ország területén belül végrehajtott megfigyelési intézkedésekre terjed ki, akkor azt ki lehetne játszani, amikor az említett harmadik ország területén kívül, az adatok továbbítás alatt állásának szakaszában alkalmaz ilyen intézkedéseket. E kockázat elkerülése érdekében a harmadik ország által biztosított védelmi szint megfelelősége értékelésének a harmadik ország jogrendjének valamennyi rendelkezésre ki kell terjednie, különösen a nemzetbiztonság területén,[105] ezek között pedig ugyanúgy szerepelnek az ország területén folyó megfigyelésre vonatkozó rendelkezések, mint azok, amelyek az e terület felé továbbítás alatt álló adatok megfigyelését teszik lehetővé.[106]

105 Lásd ebben az értelemben: Schrems ítélet (74. és 75. pont).

106 Lásd ebben az értelemben: EDPB, EU-US Privacy Shield – Second Annual Joint Review, 2019. január 22. (17. o., 86. pont).

237. Mindazonáltal senki sem vitatja, hogy – amint azt az EDPB hangsúlyozta – a védelmi szint megfelelőségének értékelése, amint az a GDPR 45. cikkének (1) bekezdéséből kitűnik, kizárólag *az adatok célországának számító harmadik ország* jogrendjének rendelkezéseire vonatkozik. Az, hogy nem lehet garantálni, hogy egy másik harmadik ország ne gyűjtse titokban ezeket az adatokat továbbításuk alatt, amint arra a Facebook Ireland, valamint az Egyesült Államok és az Egyesült Királyság kormánya hivatkozik, nem hat ki erre az értékelésre. Mindemellett az ilyen kockázat nem zárható ki azt követően sem, hogy az adatok a célországnak számító harmadik ország területére érkeztek.

238. Egyébként az is igaz, hogy a Bizottság, amikor a harmadik ország által biztosított védelmi szint megfelelőségét értékeli, adott esetben azzal szembesülhet, hogy az említett harmadik ország nem jelzi, hogy fennállnak bizonyos titkos megfigyelési programok. Ebből azonban nem következik az, hogy a*mikor ilyen programok létezéséről tájékoztatják*, akkor a Bizottság a megfelelőségi vizsgálat során eltekinthet azok figyelembevételétől. Ehhez hasonlóan, amennyiben a megfelelőségi határozat elfogadását követően az érintett harmadik ország által a területén, illetve az adatok e terület felé továbbítás alatt állása során végrehajtott bizonyos titkos megfigyelési programok fennállásáról tájékoztatják, a Bizottság köteles felülvizsgálni az e harmadik ország által biztosított védelmi szint megfelelőségére vonatkozó megállapítását, amennyiben a közlés alapján e tárgyban kétségek merülnek fel.[107]

3) A Bizottság és a kérdést előterjesztő bíróság által az Egyesült Államok joga kapcsán tett ténybeli megállapítások figyelembevételéről

239. Noha nem vitatott, hogy a Bíróságnak nincs hatásköre a harmadik ország jogának olyan értelmezésére, amely annak jogrendjében kötelező lenne, az adatvédelmi pajzsról szóló határozat érvényessége a Bizottság által az Egyesült Államok joga és gyakorlatai által azon személyek alapvető jogai tekintetében biztosított védelmi szint kapcsán végzett értékelések megalapozottságától függ, akinek adatait ebbe a harmadik országba továbbítják. A Bizottság ugyanis köteles volt megfelelőségi megállapítását megindokolni, a többek között az említett harmadik ország jogának tartalmára vonatkozó, a GDPR 45. cikkének (2) bekezdésében hivatkozott elemekre figyelemmel.[108]

240. A High Court (felsőbíróság) 2017. október 3-i ítéletében a jogvita felei által benyújtott bizonyítékok értékelését követően részletes megállapításokat ismertetett, amelyek bemutatták az amerikai jog releváns vetületeit.[109] E bemutatás nagyrészt egybevág a továbbított adatok amerikai hírszerzési hatóságok általi gyűjtésével és az azokhoz való hozzáférésükkel kapcsolatos szabályok tartalmát, illetve a jogorvoslati lehetőségeket és az e tevékenységekkel kapcsolatos felügyeleti mechanizmusokat illetően a Bizottság által az adatvédelmi pajzsról szóló határozatban tett megállapításokkal.

241. A kérdést előterjesztő bíróság, valamint több fél és a Bíróság elé észrevételt terjesztő érdekelt inkább azokat a jogkövetkezményeket kérdőjelezi meg, amelyeket a Bizottság e megállapításokra alapított – vagyis azon következtetést, amely szerint az Egyesült Államok megfelelő védelmi szintet biztosít azon személyek alapvető jogai tekintetében, akiknek adatait e határozat alapján továbbították –, nem pedig az általa az amerikai jog tartalma kapcsán benyújtott ismertetést.

107 Lásd a GDPR 45. cikkének (5) bekezdését. Lásd még: Schrems ítélet (76. pont).

108 Ily módon a „biztonságos kikötő” határozatot érvénytelennek nyilvánították, azzal az indokkal, hogy a Bizottság nem állapította meg ebben a határozatban, hogy az Egyesült Államok belföldi joga, vagy vállalt nemzetközi kötelezettségei alapján ténylegesen megfelelő védelmi szintet biztosít (Schrems ítélet, 97. pont). A Bizottság így nem állapította meg sem az érintettek alapvető jogaiba való esetleges beavatkozások korlátozására irányuló állami szabályok (Schrems ítélet, 88. pont), sem pedig az ilyen jellegű beavatkozásokkal szembeni hatékony bírói jogvédelem (Schrems ítélet, 89. pont) fennállását.

109 A jelen indítvány 54–73. pontja foglalja össze ezeket a megállapításokat.

242. E körülmények között az adatvédelmi pajzsról szóló határozat érvényességét lényegében a Bizottság által az amerikai jog tartalmát illetően tett megállapítások fényében értékelem, megvizsgálva, hogy azok igazolták-e ezen megfelelőségi határozat elfogadását.

243. Ennek kapcsán nem értek egyet azzal a DPC és M. Schrems által képviselt állásponttal, amely szerint a High Court (felsőbíróság) által az Egyesült Államok joga kapcsán tett megállapítások kötik a Bíróságot az adatvédelmi pajzsról szóló határozat érvényességének vizsgálatával összefüggésben. Az utóbbiak kifejtik, hogy mivel a külföldi jog az ír eljárási jog szerint ténybeli kérdésnek minősül, kizárólag a kérdést előterjesztő bíróság rendelkezik hatáskörrel e jog tartalmának megállapítására.

244. Az állandó ítélkezési gyakorlat kétségkívül elismeri, hogy a nemzeti bíróság rendelkezik kizárólagos hatáskörrel a releváns tények megállapítására, valamint a tagállam jogának értelmezésére és az előtte folyamatban levő jogvitára alkalmazására.[110] Ez az ítélkezési gyakorlat a Bíróság és a kérdést előterjesztő bíróság között a feladatok EUMSZ 267. cikkben kialakított eljárással összefüggő megosztásának felel meg. Míg kizárólag a Bíróság rendelkezik hatáskörrel az uniós jog értelmezésére és a másodlagos jog érvényességének megállapítására, addig az előtte fekvő konkrét ügyben dönteni kénytelen nemzeti bíróságra tartozik az ügy ténybeli és szabályozási összefüggésének megállapítása, annak érdekében, hogy a Bíróság hasznos választ tudjon nyújtani a számára.

245. A kérdést előterjesztő bíróság e kizárólagos hatáskörének indoka álláspontom szerint nem ültethető át a harmadik ország joga, mint olyan körülmény megállapítására, amely alkalmas lehet a Bíróság által egy másodlagos jogi aktus érvényességét illetően levont következtetés befolyásolására.[111] Mivel az ilyen jogi aktus érvénytelenségének megállapítása *erga omnes* hatályú az uniós jogrendben,[112] a Bíróság következtetése nem függhet az előzetes döntéshozatalra utalás eredetétől. Márpedig amint azt a Facebook Ireland és az Egyesült Államok kormánya kiemelte, az ettől függene, amennyiben a Bíróságot kötnék a kérdést előterjesztő bíróság által a harmadik ország joga kapcsán tett megállapítások, mivel azok az e megállapításokat tevő nemzeti bíróságtól függően változhatnak.

246. E megfontolásokra figyelemmel úgy vélem, hogy amennyiben egy uniós jogi aktus érvényességére vonatkozó előzetes döntéshozatalra előterjesztett kérdésre adandó válasz egy harmadik ország joga tartalmának értékelésével jár, a Bíróságot nem kötik a kérdést előterjesztő bíróság által e harmadik ország joga kapcsán tett megállapítások, noha figyelembe veheti azokat. A Bíróság adott esetben eltérhet ezektől vagy kiegészítheti őket a kontradiktórius eljárás elvének tiszteletben tartása mellett más forrásokat is figyelembe véve, annak érdekében, hogy megállapítsa a szóban forgó jogi aktus érvényességének értékeléséhez szükséges körülményeket.[113]

4) A „lényegi azonosság” standardjának tartalmáról

247. Emlékeztetek arra, hogy az adatvédelmi pajzsról szóló határozat érvényessége attól a kérdéstől függ, hogy az Egyesült Államok jogrendje azon személyek számára, akiknek az adatait az Unióból e harmadik országba továbbítják, „lényegében azonos” szintű védelmet biztosít-e azzal, amilyet a tagállamokban a GDPR és a Charta, illetve az uniós jog hatályán kívül eső területeken az EJEE-n alapuló kötelezettségvállalások alapján biztosítanak.

110 Lásd többek között: 1999. május 4-i Sürül ítélet (C-262/96, EU:C:1999:228, 95. pont); 2008. szeptember 11-i Eckelkamp és társai ítélet (C-11/07, EU:C:2008:489, 32. pont); 2016. október 26-i Senior Home ítélet (C-195/15, EU:C:2016:804, 20. pont).

111 Lásd e tekintetben a Supreme Court (legfelsőbb bíróság) 2019. május 31-i ítéletét (6.18. pont).

112 Lásd: 1981. május 13-i International Chemical Corporation ítélet (66/80, EU:C:1981:102, 12. és 13. pont).

113 Lásd e tekintetben: 2012. március 22-i GLS-ítélet (C-338/10, EU:C:2012:158, 15., 33. és 34. pont), amelyben a Bíróság egy dömpingellenes vám kivetéséről szóló rendelet érvényességének értékelése céljából figyelembe vette a Bíróság felhívására a Bizottság által benyújtott Eurostat-statisztikákat. Lásd még: 1991. október 22-i Nölle ítélet (C-16/90, EU:C:1991:402, 17. 23. és 24. pont). Ehhez hasonlóan a Schrems ítéletben (90. pont) a „biztonságos kikötő” határozat érvényességének vizsgálata során a Bíróság figyelembe vette a Bizottság egyes közleményeit.

248. Amint azt a Bíróság a Schrems ítéletben [114] hangsúlyozta, e standard nem azt jelenti, hogy a védelmi szintnek az Unióban megkövetelttel „megegyezőnek” kell lennie. Jóllehet azok az eszközök, amelyeket a harmadik ország az érintettek védelme céljából igénybe vesz, különbözhetnek azoktól az eszközöktől, amelyeket a Chartával összefüggésben értelmezett GDPR ír elő, „ezen eszközöknek a gyakorlatban […] hatékonynak kell lenniük ahhoz, hogy az Unióban biztosított védelemmel lényegében azonos védelmet biztosítsanak”.

249. Ebből álláspontom szerint az is következik, hogy a célországnak számító harmadik ország joga tükrözheti saját értékrendjét, amelynek függvényében eltérhet a különböző jelen levő érdekeknek tulajdonított súly attól, amelyet azokhoz az uniós jog rendel. Végeredményben a személyes adatok Unión belül érvényesülő védelme egy különösen magas standardnak felel meg a világ többi részében érvényes védelmi szinthez képest. A „lényegi azonosság” kritériumát tehát álláspontom szerint oly módon kell alkalmazni, hogy megőrzünk bizonyos rugalmasságot annak érdekében, hogy figyelembe vegyük az eltérő jogi és kulturális hagyományokat. E feltétel ugyanakkor azt jelenti, hacsak nem fosztjuk meg lényegétől, hogy a Chartából és az EJEE-ből fakadó alapvető jogokkal kapcsolatos egyes minimális garanciák és általános védelmi követelmények megfelelői megtalálhatók a célországnak számító harmadik ország jogrendjében. [115]

250. E tekintetben a Charta 52. cikkének (1) bekezdése értelmében a Chartában elismert jogok és szabadságok gyakorlása csak a törvény által, e jogok lényeges tartalmának tiszteletben tartásával, és az arányosság elvére figyelemmel annyiban korlátozhatók, amennyiben az elengedhetetlen, és ténylegesen az Unió által elismert valamely általános érdekű célkitűzést vagy mások jogainak és szabadságainak védelmét szolgálja. E követelmények lényegében megfelelnek az EJEE 8. cikkének (2) bekezdésében rögzítetteknek. [116]

251. A Charta 52. cikke (3) bekezdésének megfelelően, amennyiben a Charta 7., 8. és 47. cikkében garantált jogok megfelelnek az EJEE 8. és 13. cikkében szereplő jogoknak, úgy tartalmuk és terjedelmük azonos azokéval, azzal, hogy az uniós jog ugyanakkor kiterjedtebb védelmet nyújthat. Ebből a szempontból, amint az előadásomból kitűnik, a Charta 7., 8. és 47. cikkéből következő, a Bíróság által értelmezett standardok bizonyos szempontokból szigorúbbak, mint az EJEE 8. cikkéből következők, ahogy azokat az Emberi Jogok Európai Bírósága (a továbbiakban: EJEB) értelmezte.

252. Azt is megjegyzem, hogy az e bíróságok előtt folyamatban lévő egyes ügyekben arra hívják fel őket, hogy mérlegeljék újra ítélkezési gyakorlatuk egyes elemeit. Egyrészt felülvizsgálat céljából az EJEB két, az elektronikus kommunikáció megfigyelésével kapcsolatos közelmúltbeli ítéletét – a Centrüm för Rättvisa kontra Svédország ítélet [117] és a Big Brother Watch kontra Egyesült Királyság ítélet [118] – is a Nagykamara elé utalták. Másrészt három nemzeti bíróság terjesztett olyan előzetes döntéshozatal iránti kérelmeket a Bíróság elé, amelyek megnyitják a vitát arról, hogy el kell-e térnie a Tele2 Sverige ítéletből következő ítélkezési gyakorlatától. [119]

253. E pontosításokat követően most megvizsgálom az adatvédelmi pajzsról szóló határozat érvényességét a GDPR 45. cikkének a Charta és az EJEE fényében értelmezett (1) bekezdésére figyelemmel, amennyiben ezek garantálják egyrészt a magánélet tiszteletben tartásához, valamint a személyes adatok védelméhez való jogot (a b) rész), másrészt pedig a hatékony bírói jogvédelemhez való jogot (a c) rész).

114 Schrems ítélet (73. és 74. pont).

115 Lásd ebben az értelemben: 29. csoport, „Adequacy Referential (updated)”, 2017. november 28., WP 254 (3., 4. és 9. o.).

116 Az EJEE 8. cikkének (2) bekezdése ugyanakkor nem utal a magánélet tiszteletben tartásához való jog „lényeges tartalmára”. Lásd e tekintetben a jelen indítvány fenti 161. pontját.

117 EJEB, 2018. június 19. (CE:ECHR:2018:0619JUD003525208, a továbbiakban: Centrüm för Rättvisa ítélet).

118 EJEB, 2018. szeptember 13. (CCE:ECHR:2018:0913JUD005817013, a továbbiakban: Big Brother Watch ítélet).

119 Lásd a jelen indítvány 98. lábjegyzetében hivatkozott ügyeket, valamint a C-520/18. sz. Ordre des barreaux francophones et germanophones és társai ügyet.

b) Az adatvédelmi pajzsról szóló határozat érvényességéről a magánélet tiszteletben tartásához, valamint a személyes adatok védelméhez való jogra figyelemmel

254. Negyedik kérdésében a kérdést előterjesztő bíróság lényegében az Egyesült Államok által biztosított védelmi szint és az érintetteket az Unióban a magánélet tiszteletben tartásához, valamint a személyes adatok védelméhez való jog alapján megillető védelmi szint lényegi azonosságát kérdőjelezi meg.

1) A beavatkozások fennállásáról

255. Az adatvédelmi pajzsról szóló határozat (67)–(124) preambulumbekezdésében a Bizottság azon lehetőségre utal, hogy az amerikai hatóságok hozzáférjenek az Unióból továbbított adatokhoz és azokat nemzetbiztonsági célokra használják fel a különösen a FISA 702. cikkén, illetve az EO 12333-on alapuló programok keretében.

256. E programok végrehajtása olyan behatásokkal jár az amerikai hírszerzési hatóságok részéről, amelyeket, ha egy tagállam hatóságaitól erednének, a Charta 7. cikke és az EJEE 8. cikke által garantált, a magánélet tiszteletben tartásához való jog gyakorlásába való beavatkozásnak tekintenének. Azt is kifejti, hogy az érintettek annak kockázatával szembesülnek, hogy személyes adataikat a Charta 8. cikkében rögzítetteknek meg nem felelő módon fogják kezelni.[120]

257. Kiindulásként kiemelem, hogy a magánélet tiszteletben tartásához, valamint a személyes adatok védelméhez való jog nemcsak a közlések tartalmára, hanem a forgalmi adatokra[121] és helymeghatározó adatokra (a továbbiakban együtt: metaadatok) is kiterjed. Mind a Bíróság, mint az EJEB elismerte ugyanis, hogy a metaadatok a tartalmi adatokhoz hasonlóan az egyén életét illetően igen pontos információk feltárását tehetik lehetővé.[122]

258. A Bíróság ítélkezési gyakorlata szerint a Charta 7. cikkében garantált jogba történő beavatkozás fennállásának megállapítása szempontjából nem bír jelentőséggel, hogy az érintett adatok szenzitívek-e, vagy hogy az érintettnek esetlegesen származtak-e kellemetlenségei a szóban forgó megfigyelési intézkedésekből.[123]

259. Ennek felidézését követően a FISA 702. cikkén alapuló megfigyelési programok először is beavatkozásokkal járnak azon személyek alapvető jogaiba, akiknek közlései megfelelnek az NSA által megválasztott kiválasztási tényezőknek és amelyeket ebből következően az elektronikus hírközlési szolgáltatók megküldenek az utóbbinak.[124] A szolgáltatókat terhelő azon kötelezettség, hogy *bocsássák* az adatokat az NSA *rendelkezésére*, mivel eltér a közlések titkosságának elvétől,[125] önmagában

120 Noha az adatkezelés sértheti egyszerre a Charta 7. és 8. cikkét, a 8. cikk alkalmazása szempontjából releváns elemzési keret szerkezetileg eltér a 7. cikkhez kapcsolódótól. A személyes adatok védelméhez való jog a Charta 8. cikkének (2) bekezdése szerint azt jelenti, hogy „[a]z ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni”. E jog megsértése azt feltételezi, hogy a személyes adatokat e követelményeket megsértve kezelik. Ez a helyzet többek között akkor, ha az adatkezelés alapja nem az érintett személy hozzájárulása, *sem pedig más, a törvényben rögzített jogos ok*. Ilyen helyzetben, noha a beavatkozás fennállásának és igazolásának kérdése a 7. cikkel összefüggésben fogalmilag elkülönül, a Charta 8. cikke vonatkozásában ezek keverednek.

121 A 2002/58 irányelv 2. cikke második bekezdésének b) pontja úgy határozza meg a forgalmi adat fogalmát, hogy az „egy közlésnek az elektronikus hírközlő hálózaton keresztül történő továbbítása vagy erre vonatkozó számlázás céljából kezelt minden adat”.

122 Lásd: 2014. április 8-i Digital Rights Ireland és társai ítélet (C-293/12 és C-594/12, EU:C:2014:238, a továbbiakban: Digital Rights Ireland ítélet, 27. pont), valamint Tele2 Sverige ítélet (99. pont). Lásd még: EJEB, 1984. augusztus 2., Malone kontra Egyesült Királyság (CE:ECHR:1984:0802JUD000869179, 84. §) és 2018. február 8., Ben Faiza kontra Franciaország (CE:ECHR:2018:0208JUD003144612, 66. §).

123 Lásd: Digital Rights Ireland ítélet (33. pont); 1/15 vélemény (124. pont); Ministerio Fiscal ítélet (51. pont).

124 Lásd az adatvédelmi pajzsról szóló határozat (78)–(81) preambulumbekezdését, valamint VI. mellékletének II. pontját.

125 Lásd e tekintetben: Digital Rights Ireland ítélet (32. pont).

beavatkozással jár, még ha ezeket az adatokat a hírszerzési hatóságok utóbb nem is tekintik meg, illetve nem is használják fel.[126] A rendelkezésükre bocsátott közlések metaadatainak és tartalmának *tárolása* és az azokhoz való tényleges *hozzáférés* e hatóságok részéről, valamint az adatok *felhasználása* szintén további beavatkozásoknak minősülnek.[127]

260. Ezenfelül, a kérdést előterjesztő bíróság megállapításai,[128] illetve más források, mint a PCLOB FISA 702. cikke alapján végrehajtott programokról szóló, a Bírósághoz az amerikai kormány által benyújtott jelentése[129] szerint az NSA az Upstream program keretében már a távközlési „gerinchálózaton" áthaladó kommunikációáramlásban részt vevő, az NSA által megjelölt kiválasztási tényezőket nem tartalmazó közléseket hordozó adatok jelentős tömegeihez („csomagok") fért hozzá. Az NSA ezeket az adattömegeket csak annak gyors, automatizált eldöntése érdekében vizsgálhatja, hogy tartalmazzák-e az említett kiválasztási tényezőket. Kizárólag az ily módon megszűrt közléseket tárolják ezt követően az NSA adatbázisaiban. Az adatokhoz való ezen hozzáférés, azok szűrése céljából, álláspontom szerint szintén beavatkozásnak minősül az érintett személyek magánélet tiszteletben tartásához való jogának gyakorlásába, függetlenül attól, hogy a tárolt adatokat utóbb mire használják.[130]

261. Egyébként a szóban forgó adatok rendelkezésre bocsátása és szűrése,[131] az ezen adatokhoz való hozzáférés a hírszerzési hatóságok részéről, valamint az említett adatok esetleges tárolása, elemzése és felhasználása a GDPR 4. cikke (2) bekezdésének, valamint a Charta 8. cikke (2) bekezdésének értelmében vett adatkezelés körébe tartozik. Ezeknek az adatkezeléseknek tehát meg kell felelniük az utóbbi rendelkezés által előírt követelményeknek.[132]

262. Az EO 12333-on alapuló megfigyelés az államterület felé továbbítás alatt álló adatokhoz való közvetlen hozzáféréssel járhat a hírszerzési hatóságok részéről, ezáltal az EJEE 8. cikkében garantált jog gyakorlásába való beavatkozást vonva maga után. E beavatkozáshoz csatlakozik az említett adatok esetleges utóbbi felhasználása által megvalósított beavatkozás.

2) A beavatkozások „törvényben rögzítettségéről"

263. A Bíróság[133] és az EJEB[134] ítélkezési gyakorlata értelmében az a követelmény, hogy az alapvető jogok gyakorlásába való bármely beavatkozást a Charta 52. cikke (1) bekezdésének, valamint 8. cikke (2) bekezdésének értelmében „törvényben kell rögzíteni", nem csak azt jelenti, hogy a beavatkozást előíró intézkedésnek törvényi alappal kell rendelkeznie a belső jogban, hanem azt is, hogy e törvényi alapnak bizonyos hozzáférhetőségi és előreláthatósági tulajdonságokkal kell rendelkeznie az önkényesség kockázatának elkerülése érdekében.

264. E tekintetben a felek és a Bíróság elé észrevételt terjesztő érdekeltek között lényegében azzal kapcsolatban van vita, hogy a FISA 702. cikke és az EO 12333 megfelelnek-e a törvény előreláthatóságára vonatkozó feltételnek.

126 Lásd ebben az értelemben: 1/15 vélemény (124. és 125. pont), amelyből kitűnik, hogy az adatok harmadik személlyel történő közlése az érintettek alapvető jogába történő beavatkozásnak minősül, függetlenül attól, hogy azokat utóbb mire használják.

127 Lásd ebben az értelemben: Digital Rights Ireland ítélet (35. pont); Schrems ítélet (87. pont); 1/15 vélemény (123–126. pont).

128 Lásd a jelen indítvány 60. pontját.

129 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA], 2014. július 2. (a továbbiakban: PCLOB-jelentés, 84. és 111. o.). Lásd még: 29. csoport, EU-U. S. Privacy Shield – First Annual Joint Review, 2017. november 28., WP 255 (B.1.1. pont, 15. o.).

130 Lásd a jelen indítvány 126. lábjegyzetét.

131 Lásd e tekintetben a jelen indítvány 222. pontját.

132 Lásd: 1/15 vélemény (123. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

133 Lásd többek között: 1/15 vélemény (146. pont).

134 Lásd többek között: EJEB, 1984. augusztus 2., Malone kontra Egyesült Királyság (CE:ECHR:1984:0802JUD000869179, 66. §); 2006. június 29-i Weber és Saravia kontra Németország határozat (CE:ECHR:2006:0629DEC005493400, a továbbiakban: Weber és Saravia határozat, 84. §, valamint az ott hivatkozott ítélkezési gyakorlat); 2015. december 4-i Zakharov kontra Oroszország ítélet (CE:ECHR:2015:1204JUD004714306, a továbbiakban: Zakharov ítélet, 228. §).

265. Ez a Bíróság[135] és az EJEB[136] által értelmezett feltétel azt követeli meg, hogy a magánélet tiszteletben tartásához való jog gyakorlásába történő beavatkozást tartalmazó szabályozásnak egyértelmű és pontos szabályokat kell tartalmaznia a szóban forgó intézkedés hatálya és alkalmazása vonatkozásában, és minimális követelményeket kell előírnia, oly módon, hogy az érintettek elegendő olyan biztosítékkal rendelkezzenek, amely lehetővé teszi az adataiknak a visszaélések veszélyeivel, valamint az azokat érintő minden jogellenes hozzáféréssel és felhasználással szembeni védelmét. E szabályoknak meg kell jelölniük, hogy e személyes adatok hatóságok általi megőrzése, valamint az azokhoz való hozzáférés és azok felhasználása milyen körülmények között és milyen feltételek alapján lehetséges.[137] Egyébként a beavatkozást lehetővé tevő jogalapnak magának kell meghatároznia a magánélet tiszteletben tartásához való jog gyakorlásával kapcsolatos korlátozás terjedelmét.[138]

266. M. Schrems-hez és az EPIC-hez hasonlóan kétlem, hogy az EO 12333 és a valamennyi jelfelderítési tevékenységhez kapcsolódóan garanciákat rögzítő PPD 28[139] kellően előrelátható ahhoz, hogy törvénynek minősüljön.

267. E jogi aktusok kifejezetten rögzítik, hogy nem ruháznak jogilag érvényesíthető jogokat az érintettekre.[140] Azok tehát nem hivatkozhatnak a PPD 28 által előírt garanciákra bíróság előtt.[141] A Bizottság egyébként az adatvédelmi pajzsról szóló határozatban úgy tekintette, hogy az ezen elnöki irányelvben rögzített garanciák, noha kötelező jellegűek a hírszerző szolgálatokra nézve,[142] „nem ezzel a jogi kifejezéssel éltek [helyesen: nem jogi formában vannak megfogalmazva]”.[143] Az EO 12333 és a PPD 28 inkább olyan belső közigazgatási utasításoknak tűnnek, amelyeket az Egyesült Államok elnöke visszavonhat vagy módosíthat. Márpedig az EJEB már kimondta, hogy a belső közigazgatási irányelvek nem minősülnek törvénynek.[144]

268. Ami a FISA 702. cikkét illeti, e rendelkezés előreláthatóságát M. Schrems arra hivatkozva kérdőjelezi meg, hogy az az adatok szűrése céljából használt kiválasztási tényezők megválasztásához nem rendel megfelelő garanciákat a visszaélés veszélyével szemben. Mivel a problémakör a FISA 702. cikkében előírt beavatkozások szigorúan szükséges jellegét is érinti, azt indítványom későbbi részében vizsgálom meg azt.[145]

135 Lásd többek között: Digital Rights Ireland ítélet (54. és 65. pont); Schrems ítélet (91. pont); Tele2 Sverige ítélet (109. pont); 1/15 vélemény (141. pont).

136 Lásd többek között: Weber és Saravia határozat (94. és 95. §); Zakharov ítélet (236. §), valamint EJEB, 2016. január 12., Szabó és Vissy kontra Magyarország (CE:ECHR:2016:0112JUD003713814, a továbbiakban: Szabó és Vissy ítélet, 59. §).

137 Lásd: Tele2 Sverige ítélet (117. pont), valamint 1/15 vélemény (190. pont). Lásd még többek között: EJEB, 1984. augusztus 2., Malone kontra Egyesült Királyság (CE:ECHR:1984:0802JUD000869179, 67. §); Zakharov ítélet (229. §); Szabó és Vissy ítélet (62. §). AZ EJEB itt kimondja, hogy az előreláthatóság követelményének nem lehet ugyanolyan tartalma a kommunikáció megfigyelésének területén, mint más területeken. A titkos megfigyelési intézkedésekkel összefüggésben „[a]z előreláthatóság […] nem jelenti azt, hogy az egyénnek előre tudnia kell a hatóságok valószínű megfigyelési tevékenységéről, hogy így ehhez igazíthassa a viselkedését”.

138 1/15 vélemény (139. pont). Lásd még ebben az értelemben: EJEB, 1983. március 25., Silver és társai kontra Egyesült Királyság (CE:ECHR:1983:0325JUD000594772, 88. és 89. §).

139 Az adatvédelmi pajzsról szóló határozat (69)–(77) preambulumbekezdése, valamint VI. mellékletének I. pontja tartalmazza a PPD 28 ismertetését. Ebben az szerepel, hogy ez az elnöki irányelv mind a FISA 702. cikkén alapuló, mind az Egyesült Államok területén kívül végzett hírszerzési tevékenységre alkalmazandó.

140 Az EO 12333 3.7. pontjának c) alpontja a következőket mondja ki: „[t]his order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person”. A PPD 28 6. cikkének d) pontja is a következőket írja elő: „This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person”.

141 Lásd ebben az értelemben: EDPB, EU-U. S. Privacy Shield – Second Annual Joint Review, 2019. január 22. (99. pont).

142 Lásd az adatvédelmi pajzsról szóló határozat (69)–(77) preambulumbekezdését.

143 Az adatvédelmi pajzsról szóló határozat (76) preambulumbekezdése.

144 Lásd: EJEB, 1983. március 25., Silver és társai kontra Egyesült Királyság (CE:ECHR:1983:0325JUD000594772, 26. és 86. §).

145 Lásd a jelen indítvány 295–301. pontját. A Tele2 Sverige ítélet (116. és 117. pont), valamint az 1/15 vélemény (140. és 141. pont) a törvény előreláthatóságának feltételét úgy mutatta be, mint amely szervesen kapcsolódik a beavatkozás szükségességének és arányosságának feltételéhez. Ugyanígy az EJEB ítélkezési gyakorlata szerint a visszaélés kockázataival szembeni hatékony garanciák fennállása a beavatkozás „előreláthatóságára” vonatkozó feltételnek, valamint az „egy demokratikus társadalomban szükséges” jellegére vonatkozó feltételnek része: e két feltétel tiszteletben tartását együttesen kell megvizsgálni. Lásd többek között: EJEB, 2010. május 18., Kennedy kontra Egyesült Királyság (CE:ECHR:2010:0518JUD002683905, 155. §); Zakharov ítélet (236. §); Centrüm för Rättvisa ítélet (107. §); Big Brother Watch ítélet (322. §).

269. Az előzetes döntéshozatalra előterjesztett harmadik kérdés átfedésben van a „törvényi minőségre” vonatkozó feltétel tiszteletben tartásával. E kérdéssel a kérdést előterjesztő bíróság lényegében azt kívánja megtudni, hogy a harmadik országban biztosított védelmi szint megfelelőségét kizárólag az e harmadik országban hatályos jogilag kötelező szabályokra és az azok tiszteletben tartásának biztosítására irányuló gyakorlatokra figyelemmel kell-e megvizsgálni, vagy a különböző ott alkalmazott nem kötelező aktusokat és bíróságon kívüli felülvizsgálati mechanizmusokat is figyelembe kell venni.

270. E tárgyban a GDPR 45. cikke (2) bekezdésének a) pontja tartalmazza azon körülmények nem kimerítő listáját, amelyeket a Bizottságnak figyelembe kell vennie a harmadik ország által nyújtott védelem megfelelőségének értékelése céljából. E körülmények között szerepelnek az alkalmazandó jogszabályok, valamint azok végrehajtásának módja. E rendelkezés utal más normatípusok, így a szakmai szabályok és biztonsági intézkedések hatására is. Ezenkívül előírja a „tényleges és érvényesíthető [jogok]”, valamint „az [érintetteket], akiknek a személyes adatait továbbítják, [megillető] hatékonyan érvényesíthető […] közigazgatási és bírósági [jogorvoslatok]” figyelembevételét. [146]

271. Összességében értelmezve, a rendeletben található lista nem teljeskörű jellegére is figyelemmel az említett rendelkezés álláspontom szerint azt jelenti, hogy a nem valamely elérhető és előrelátható jogalapra alapított gyakorlatok és aktusok figyelembe vehetők a szóban forgó harmadik ország által nyújtott védelmi szint összesített értékelése során, oly módon, hogy azok megerősítik az ilyen jellegű jogalapokon alapuló garanciákat. Ezzel szemben, amint azt lényegében a DPC, M. Schrems az osztrák kormány és az EDPB kifejtik, az ilyen aktusok vagy gyakorlatok nem helyettesíthetik az ilyen garanciákat, és így maguk nem biztosíthatják a megkövetelt védelmi szintet.

3) Az alapvető jogok lényeges tartalma megsértésének hiányáról

272. A Charta 52. cikkének (1) bekezdésében rögzített azon követelmény, amely szerint a Chartában garantált jogok és szabadságok gyakorlása csak e jogok lényeges tartalmának tiszteletben tartásával korlátozható, azt jelenti, hogy amennyiben a beavatkozás ezt sérti, az semmilyen jogszerű céllal nem igazolható. A beavatkozást ilyenkor a Chartával ellentétesnek tekintik, anélkül hogy meg kellene vizsgálni, hogy alkalmas és szükséges-e a követett cél elérésére.

273. Ennek kapcsán a Bíróság kimondta, hogy az olyan szabályozás, amely lehetővé teszi a hatóságok számára, hogy általános jelleggel hozzáférjenek az elektronikus közlések *tartalmához*, a Charta 7. cikkében biztosított magánélet tiszteletben tartásához való jog lényegét sérti. [147] Ezzel szemben hangsúlyozva a *forgalmi és helymeghatározó adatokhoz* való hozzáféréshez és azok elemzéséhez kapcsolódó kockázatokat, [148] a Bíróság úgy ítélte meg, hogy e jog lényeges tartalmát nem érinti, ha a nemzeti szabályozás általános jelleggel hozzáférést enged a hatóságok számára ezen adatokhoz. [149]

146 Lásd továbbá a GDPR (104) preambulumbekezdését.

147 Lásd: Schrems ítélet (94. pont). Lásd még: Digital Rights Ireland ítélet (39. pont), valamint Tele2 Sverige ítélet (101. pont). Figyelemmel a magánélet tiszteletben tartásához való jog és a személyes adatok védelméhez való jog közötti szoros kapcsolatra, a hatóságok számára a közlések tartalmához általános jelleggel hozzáférést biztosító nemzeti intézkedés álláspontom szerint a Charta 8. cikkében rögzített jog lényeges tartalmát is sértené.

148 Lásd a jelen indítvány 257. pontját. A Tele2 Sverige ítéletben (99. pont) a Bíróság kiemelte, hogy a metaadatok közelebbről eszközül szolgálnak az érintett személyek profiljának megalkotásához. Az elektronikus kommunikáció hírszerzési és nemzetbiztonsági célokból történő megfigyeléséről szóló, 2014. április 10-i 04/2014. sz. véleményében (WP 215, 5. o.) a 29. csoport megjegyezte, hogy strukturált jellegük miatt a metaadatokat könnyebb összesíteni és elemezni, mint a tartalmi adatokat.

149 Lásd: Tele2 Sverige ítélet (99. pont). Egyes kommentátorok a technológia és a kommunikációs módszerek fejlődésére figyelemmel megkérdőjelezték a közlések tartalmához való általános jellegű hozzáférés és a metaadatokhoz való általános jellegű hozzáférés közötti megkülönböztetés megalapozottságát. Lásd Falot, N. és Hijmans, H., „Tele2: de afweging tussen privacy en veiligheid nader omlijnd”, *Nederlands Tijdschrift voor Europees Recht*, 3. sz., 2017 (48. o.), valamint Ojanen, T., „Making essence of the rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter” (a Schrems ítélet kommentárja), *European Constitutional Law Review*, 2016 (5. o.).

274. A FISA 702. cikkét álláspontom szerint nem lehet úgy tekinteni, mint amely általános jellegű hozzáférést engedélyez az amerikai hírszerzési hatóságok számára az elektronikus közlések tartalmához.

275. Egyrészt ugyanis a FISA 702. cikke alapján a hírszerzési hatóságok adatokhoz való hozzáférése *azok esetleges elemzése és felhasználása céljából* az egyedi célpontokhoz kapcsolódó kiválasztási tényezőknek megfelelő adatokra korlátozódik.

276. Másrészt az Upstream program vitathatatlanul általános jellegű hozzáférést eredményezhetne az elektronikus közlések tartalmához *azok automatikus szűrése céljából*, amennyiben a kiválasztási tényezőket nem kizárólag a „honnan" és „hová" mezőkre alkalmaznák, hanem az áramlás tartalmának egészére (a szelekciós tényezővel „kapcsolatos" keresés).[150] Ugyanakkor, amint azt a Bizottság előadja, ellentétben M. Schrems és az EPIC állításával, a hírszerzési hatóságok ideiglenes hozzáférése az elektronikus közlések teljes tartalmához, kizárólag azok kiválasztási tényezők révén történő szűrése céljából, nem tekinthető az e tartalomhoz való általános jellegű hozzáférésnek.[151] Álláspontom szerint ebből az időben az automatikus szűrés céljaira korlátozott hozzáférésből következő beavatkozás súlyossága nem éri el azon beavatkozás súlyosságát, amely a hatóságok e tartalomhoz való általános jellegű hozzáféréséből következik, annak elemzése és esetleges felhasználása céljából.[152] A szűrés célját szolgáló ideiglenes hozzáférés nem teszi lehetővé e hatóságok számára a közlések olyan metaadatainak vagy tartalmának tárolását, amelyek nem felelnek meg a kiválasztási tényezőknek, és különösen azt nem, amint azt az amerikai kormány megjegyzi, hogy profilokat alkossanak az e kritériumok által meg nem célzott egyénekről.

277. Mindezek alapján a kiválasztási tényezők megválasztásának keretétől függ az a kérdés, hogy a FISA 702. cikkén alapuló, kiválasztási tényezők révén elért személyre irányultság ténylegesen korlátozza-e a hírszerzési hatóságok hatásköreit.[153] M. Schrems e tekintetben előadja, hogy az ezzel kapcsolatos megfelelő ellenőrzés hiányában az amerikai jog nem ír elő garanciát a közlések tartalmához való általános jellegű hozzáféréssel szemben már a szűrés szakaszában és az ily módon az érintettek magánélet tiszteletben tartásához való jogának lényegét sérti.

278. Amint azt lent részletesebben kifejtem,[154] hajlok arra, hogy egyetértsek e kétségekkel a kiválasztási tényezők megválasztási keretének elégséges jellegét illetően, a beavatkozások előreláthatóságával és arányosságával kapcsolatos feltételeknek való megfelelés szempontjából. E keret létezése azonban – még ha nem is tökéletes – kizárja azt a következtetést, amely szerint a FISA 702. cikke az elektronikus közlések tartalmához való általános jellegű hozzáférést engedélyez a hatóságok számára, és ennélfogva egyenértékű a Charta 7. cikkében rögzített jog lényegének megsértésével.

150 Lásd az adatvédelmi pajzsról szóló határozat 87. lábjegyzetét. Ugyanakkor az EPIC észrevételei, illetve az Egyesült Államok kormánya által a Bíróság kérdéseire adott írásbeli válasz szerint a FISC 2017-ben a kiválasztási tényezővel „kapcsolatos" keresések felfüggesztését írta elő, az ilyen típusú kereséseket érintő szabálytalanságok miatt. A Kongresszus azonban a FISA-t ismételten engedélyező, 2018-ban elfogadott jogi aktusban rögzítette az ilyen típusú keresés ismételt bevezetésének lehetőségét, a FISC és a Kongresszus hozzájárulásával. Lásd még: EDPB, EU-U. S. Privacy Shield – Second Annual Joint Review, 2019. január 22. (27. o., 55. pont).

151 Ebből a szempontból a kérdést előterjesztő bíróság 2017. október 3-i ítéletének 188. és 189. pontjában megkülönbözteti a „tömeges" keresést, az adatok „tömeges" megszerzésétől, gyűjtésétől, illetve tárolásától. E bíróság lényegében úgy ítéli meg, hogy bár az Upstream program „tömeges" kereséssel jár a távközlési „gerinchálózaton" áthaladó adatáramlás egészében, az adatok megszerzése, gyűjtése és tárolása célzott abban az értelemben, hogy azok tárgyát kizárólag a szóban forgó kiválasztási tényezőket tartalmazó adatok képezik.

152 Lásd ebben az értelemben: a Supreme Court (legfelsőbb bíróság) 2019. május 31-i ítélete (1.12. és 1.13. pont). E bíróság e pontokban a következőket emeli ki: „[I]t is inevitable that any screening process designed to identify data of interest will necessarily involve all of the data available, for the whole point of the screening process is to identify within that entire universe of available data the relevant material which may be of interest and thus require closer scrutiny. Perhaps part of the problem lies in the fact that the term »processing« covers a wide range of activity, apparently, in the view of the DPC, including screening. On the assumption that that is a correct view of the law, then it is technically correct to describe bulk screening as involving indiscriminate processing. But the use of that terminology might be taken to imply that other forms of processing, which are significantly more invasive, are carried out on an indiscriminate basis."

153 Lásd: 1/15 vélemény (122. pont). Lásd még a Jog a Demokráciáért Európai Bizottság (Velencei Bizottság) 2015. december 15-i jelentését a jelfelderítési információkat gyűjtő ügynökségek demokratikus ellenőrzéséről, 719/2013. sz. tanulmány, (CDL-AD(2015)011, 11. o.): „A gyakorlatban az a kérdés, hogy e folyamat megfelelően korlátozza-e a felesleges beavatkozásokat az ártalmatlan személyes közlésekbe, annak eldöntéséhez vezet, hogy a kiválasztási tényező kellően releváns és konkrét-e, valamint hogy a kiválasztott paraméterek keretében a releváns adatok azonosítására alkalmazott szoftver algoritmusának minősége kielégítő-e […]".

154 Lásd a jelen indítvány 297–301. pontját.

279. Azt is hangsúlyozom, hogy 1/15 véleményében a Bíróság úgy ítélte meg, hogy a személyes adatok védelméhez való, a Charta 8. cikkében biztosított jog lényeges tartalma akkor nem sérül, ha az adatkezelés céljai meghatározottak és ahhoz többek között az adatok biztonságának, titkosságának és sértetlenségének biztosítását, valamint jogellenes hozzáféréssel és kezelésekkel szembeni védelmét célzó szabályok kapcsolódnak.[155]

280. Az adatvédelmi pajzsról szóló határozatban a Bizottság megállapította, hogy mind a FISA 702. cikke, mind pedig a PPD 28 körülhatárolja azon célokat, amelyek érdekében az adatokat a FISA 702. cikke alapján végrehajtott programok keretében gyűjteni lehet.[156] A Bizottság e határozatban arra is rámutatott, hogy a PPD 28 az adatokhoz való hozzáférést, valamint tárolásukat és terjesztésüket meghatározó szabályokat ír elő, az adatok biztonságának biztosítása és az engedély nélküli hozzáférés megakadályozása céljából.[157] Amint azt a későbbiekben kifejtem,[158] különösen azzal kapcsolatban vannak kétségeim, hogy a szóban forgó adatkezelések céljai kellő egyértelműséggel és pontossággal vannak-e meghatározva ahhoz, hogy lényegében azonos védelmi szintet biztosítsanak az uniós jogrendben érvényesülővel. Ezek az esetleges hiányosságok azonban álláspontom szerint nem alapozzák meg azt a megállapítást, amely szerint az ilyen programok, ha azokat az Unión belül hajtanák végre, sértenék a személyes adatok védelméhez való jog lényeges tartalmát.

281. Egyebekben emlékeztetek arra, hogy az EO 12333-on alapuló megfigyelési tevékenységekkel összefüggésben biztosított védelmi szint megfelelőségét az EJEE rendelkezései alapján kell értékelni. Ennek kapcsán az adatvédelmi pajzsról szóló határozatból kitűnik, hogy a nem amerikai személyekre vonatkozó adatok gyűjtését célzó, az EO 12333-on alapuló intézkedések végrehajtása kapcsán érvényesülő korlátozásokat egyedül a PPD 28 tartalmazza.[159] Ez az elnöki irányelv azt mondja ki, hogy a külföldi hírszerzési információk felhasználásának „a lehető legcélzottabbnak kell lennie”. Kifejezetten utal ugyanakkor az amerikai területen kívüli a „tömeges” adatgyűjtés lehetőségére, egyes konkrét nemzetbiztonsági célok elérése érdekében.[160] M. Schrems álláspontja szerint a magánszemélyek számára jogokat egyébként nem keletkeztető PPD 28 rendelkezései nem nyújtanak védelmet az érintettek számára az elektronikus közléseik tartalmához való általános jellegű hozzáférésekkel szemben.

155 1/15 vélemény (150. pont).

156 Lásd az adatvédelmi pajzsról szóló határozat (70), (103) és (109) preambulumbekezdését.

157 Lásd az adatvédelmi pajzsról szóló határozat (83)–(87) preambulumbekezdését, valamint VI. melléklete I. pontjának c) alpontját. Megjegyzem, hogy a PCLOB jelentése (51–66. pont) szerint az NSA FISA 702. cikkén alapuló „adattakarékossági” eljárásainak legtöbb vetülete csak az amerikai személyeket érinti. A PPD 28 ki kívánta kiterjeszteni az alkalmazandó garanciákat a nem amerikai személyekre. Lásd PCLOB, Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities, elérhető: https://www.pclob.gov/reports/report-PPD28/ (2. o.). Mindezek alapján az adatok – azok hatóságok általi megszerzését követő – nemzetbiztonsági célú tárolása és felhasználása álláspontom szerint nem tartozik az uniós jog hatálya alá (lásd a jelen indítvány 226. pontját). Az e tevékenységekkel összefüggésben biztosított védelmi szint megfelelőségét tehát csak az EJEE 8. cikkére figyelemmel kell értékelni.

158 Lásd a jelen indítvány 283–289. pontját.

159 A Bizottság így az adatvédelmi pajzsról szóló határozat (127) preambulumbekezdésében megállapította, hogy az Egyesült Államok Alkotmányának negyedik kiegészítése nem alkalmazandó a nem amerikai személyekre.

160 Lásd az adatvédelmi pajzsról szóló határozat (73) és (74) preambulumbekezdését, valamint VI. melléklete I. pontjának b) alpontját. E célok közé tartozik a kémkedés, valamint a külföldi hatalmak Egyesült Államok és érdekei ellen irányuló egyéb fenyegetései és tevékenységei ellen irányuló küzdelem; a terrorista fenyegetések elleni küzdelem; a tömegpusztító fegyverek fejlesztéséből, birtoklásából, elterjedéséből vagy felhasználásából eredő fenyegetések elleni küzdelem; a kiberbiztonsághoz kapcsolódó fenyegetések elleni küzdelem; az Egyesült Államok vagy szövetségesei fegyveres erőit érintő fenyegetések elleni küzdelem; valamint a nemzetközi bűnözés fenyegetései elleni küzdelem. A PPD 28 5. lábjegyzete szerint a „tömegesen” gyűjtött adatok felhasználását igazoló célok korlátozása nem érvényesül akkor, ha az ilyen adatgyűjtés pusztán ideiglenes és a célzott adatgyűjtés megkönnyítését célozza.

282. E tárgyban pusztán annyit jegyzek meg, hogy az EJEB az EJEE 8. cikkére vonatkozó ítélkezési gyakorlatában nem alkalmazta a magánélet tiszteletben tartásához való jog lényeges tartalma, illetve lényege megsértésének fogalmát.[161] E bíróság mindeddig nem tekintette úgy, hogy az elektronikus közlések akár tömeges megfigyelését lehetővé tévő rendszerek ö*nmagukban túllépnek a tagállamok mérlegelési mozgásterén*. Az EJEB úgy véli, hogy az ilyen rendszerek összeegyeztethetők az EJEE 8. cikkének (2) bekezdésével, amennyiben azokhoz bizonyos számú minimális garancia kapcsolódik.[162] E körülmények között álláspontom szerint nem lenne helyes azt megállapítani, hogy az EO 123333-ban előírthoz hasonló megfigyelési rendszer túllép a tagállamok mérlegelési mozgásterén anélkül, hogy valamilyen módon megvizsgálnánk az ahhoz kapcsolódó garanciákat.

4) A jogszerű cél követéséről

283. A Charta 52. cikkének (1) bekezdése szerint a Chartában rögzített jogok korlátozásának ténylegesen meg kell felelnie valamely az Unió által elismert általános érdekű célkitűzésnek. A Charta 8. cikkének (2) bekezdése azt is kimondja, hogy a személyes adatok olyan kezelésének, amelynek alapja nem az érintett személy hozzájárulása, „a törvényben rögzített jogos [okon]" kell alapulnia. Az EJEE 8. cikkének (2) bekezdése felsorolja azokat a célokat, amelyek igazolhatják a beavatkozását a magánélet tiszteletben tartásához való jog gyakorlásába.

284. Az adatvédelmi pajzsról szóló határozat értelmében a határozatban rögzített elvekhez való csatlakozás korlátozható nemzetbiztonsággal, a közérdekkel és a törvény tiszteletben tartásával kapcsolatos kötelezettségek teljesítése céljából.[163] E határozat (67)–(124) preambulumbekezdése vizsgálja meg konkrétabban azokat a korlátozásokat, amelyek abból fakadnak, hogy az amerikai hatóságok nemzetbiztonsági célokból hozzáférnek az adatokhoz és felhasználják azokat.

285. Nem vitatott, hogy a nemzetbiztonság védelme olyan jogszerű célnak minősül, amely igazolhatja az eltérést a GDPR-en alapuló követelményektől,[164] valamint a Charta 7. és 8. cikkében,[165] illetve az EJEE 8. cikkének (2) bekezdésében rögzített jogoktól. M. Schrems, az osztrák kormány és az EPIC ugyanakkor megjegyezték, hogy a FISA 702. cikkére, valamint az EO 12333-ra alapított megfigyelési programok keretében követett célok túllépnek a puszta nemzetbiztonságon. E jogi aktusok célja ugyanis „külföldi hírszerzési információk" szerzése: e fogalom különböző típusú információkat takar, beleértve a nemzetbiztonságra vonatkozó információkat is, de nem korlátozódik szükségképpen ezekre.[166] Ily módon a FISA 702. cikke értelmében vett külső hírszerzési információk közé tartoznak a külüggyel

161 Noha az EJEE rendelkezései nem utalnak az alapvető jogok „lényeges tartalmára", az azzal egyenértékű alapvető jog „lényegének" fogalma megjelenik az EJEB egyes ilyen rendelkezésekkel kapcsolatos ítélkezési gyakorlatában. Lásd az EJEE 6. cikkében garantált tisztességes tárgyaláshoz való jog lényegét illetően: EJEB, 1985. május 25., Ashingdane kontra Egyesült Királyság (CE:ECHR:1985:0528JUD000822578, 57. és 59. §); 2000. december 21., Heaney és McGuinness kontra Írország (CE:ECHR:2000:1221JUD003472097, 55. és 58. §); valamint 2016. június 23., Baka kontra Magyarország (CE:ECHR:2016:0623JUD002026112, 121. §). Az EJEE 12. cikkében rögzített házasságkötéshez való jog lényegét illetően lásd: EJEB, 2002. július 11., Christine Goodwin kontra Egyesült Királyság (CE:ECHR:2002:0711JUD002895795, 99. és 101. §). Az EJEE 1. kiegészítő jegyzőkönyvében szereplő oktatáshoz való jog lényegét illetően lásd: EJEB, 1968. július 23., a belga nyelvi kérdés ügye (CE:ECHR:1968:0723JUD000147462, 5. §).

162 Lásd különösen Centrüm för Rättvisa ítélet (112–114. §, valamint az ott hivatkozott ítélkezési gyakorlat) és Big Brother Watch ítélet (337. §).

163 Lásd a jelen indítvány 197. pontját.

164 Lásd a GDPR 23. cikke (1) bekezdésének a) pontját.

165 Lásd: Schrems ítélet (88. pont). A Bíróság úgy ítélte meg, hogy az EUMSZ rendelkezéseinek értelmében vett „közbiztonság" szomszédos fogalma, mint az uniós jognak a tagállamok belső és külső biztonságát is lefedő önálló fogalma megengedi az EUMSZ által garantált alapvető szabadságoktól való eltérést (lásd többek között: 1999. október 26-i Sirdar ítélet [C-273/97, EU:C:1999:523, 17. pont]; 2016. szeptember 13-i CS ítélet [C-304/14, EU:C:2016:674, 39. pont, valamint az ott hivatkozott ítélkezési gyakorlat]). Míg a belső biztonságra hatással lehet például az érintett tagállam népessége nyugalmának és fizikai biztonságának közvetlen veszélyeztetése, addig a külső biztonságot többek között a külkapcsolatok vagy a nemzetek békés egymás mellett élése komoly megzavarásának a kockázata veszélyeztetheti. Anélkül, hogy egyoldalúan meghatározhatnák e fogalmak tartalmát, az egyes tagállamok bizonyos mérlegelési mozgástérrel rendelkeznek lényeges biztonsági érdekeik meghatározása terén. Lásd különösen: 2018. május 2-i K. és H. F. ítélet (Tartózkodáshoz való jog és háborús bűncselekmények gyanúja) (C-331/16 és C-366/16, EU:C:2018:296, 40–42. pont, valamint az ott hivatkozott ítélkezési gyakorlat). E megfontolások álláspontom szerint átültethetők a „nemzetbiztonság", mint olyan érdek fogalmának értelmezésére, amelynek védelme igazolhatja a GDPR rendelkezéseit, valamint a Charta 7. és 8. cikkében garantált jogokat érintő korlátozásokat.

166 Lásd e tekintetben az adatvédelmi pajzsról szóló határozat (89) preambulumbekezdését és 97. lábjegyzetét.

kapcsolatos információk.[167] Az EO 12333 e fogalmat úgy határozza meg, hogy az a külföldi kormányok, külföldi szervezetek, illetve külföldi személyek képességeivel, szándékaival, illetve tevékenységeivel kapcsolatos információkra terjed ki.[168] M. Schrems megkérdőjelezi az ily módon hivatkozott cél jogszerűségét, mivel az túlmegy a nemzetbiztonságon.

286. Álláspontom szerint a külügyekkel kapcsolatos érdekek védelme bizonyos mértékig a nemzetbiztonság körébe tartozhat.[169] Egyébként elképzelhető, hogy a FISA 702. cikkében, valamint az EO 12333-ban meghatározott külső hírszerzési információk fogalma alá tartozó, a nemzetbiztonság védelmétől eltérő egyes célok megfelelnek a magánélet tiszteletben tartásához való jogba és a személyes adatok védelméhez való jogba történő beavatkozás igazolására alkalmas általános érdekű célkitűzéseknek. Az érintettek alapvető jogai és a beavatkozás által elérni kívánt cél mérlegelése során e célok mindenféleképpen kisebb súlyt képviselnek, mint a nemzetbiztonság megóvása.[170]

287. Ugyanakkor a Charta 52. cikke (1) bekezdésének megfelelően még az is szükséges, hogy a szóban forgó beavatkozásokat előíró intézkedések ténylegesen a nemzetbiztonság célját vagy egy másik jogszerű célt kövessenek.[171] Ezenkívül a beavatkozások céljait oly módon kell meghatározni, amely megfelel a világosság és az egyértelműség követelményeinek.[172]

288. Márpedig M. Schrems szerint a FISA 702. cikkében, valamint az EO 12333-ban előírt megfigyelési intézkedések célját nem jelölik meg kellően pontosan ahhoz, hogy biztosított legyen az előreláthatóság és az arányosság garanciájának tiszteletben tartása. Ez különösen annyiban igaz, amennyiben e jogi aktusok a külső hírszerzési információk fogalmát rendkívül szélesen határozzák meg. Ezenfelül a Bizottság az adatvédelmi pajzsról szóló határozat (109) preambulumbekezdésében azt állapította meg, hogy a FISA 702. cikke azt követeli meg, hogy a külső hírszerzési információk gyűjtése az adatgyűjtés „jelentős céljának” minősüljön, e megfogalmazás pedig első ránézésre nem zárja ki más, meg nem határozott célok követését, amint arra az EPIC is rámutatott.

289. A fenti okok miatt – anélkül, hogy kizárt lenne, hogy a FISA 702. cikkén, valamint az EO 12333-on alapuló megfigyelési intézkedések jogszerű céloknak felelnek meg– felmerülhet a kérdés, hogy azok kellően egyértelműen és pontosan vannak-e meghatározva a visszaélés veszélyének elkerüléséhez, illetve ahhoz, hogy lehetővé tegyék az azokból fakadó beavatkozások arányosságával kapcsolatos vizsgálatot.[173]

167 Lásd a jelen indítvány 55. pontját.

168 Lásd a jelen indítvány 61. pontját.

169 A Centrüm för Rättvisa ítéletben (111. §) az EJEB kimondta, hogy a Svédország külpolitikájának, védelempolitikájának és biztonságpolitikájának támogatását, valamint a Svédországban szervezett külső fenyegetések azonosítását célzó megfigyelési intézkedések a nemzetbiztonsággal kapcsolatos jogszerű célokat követnek.

170 Lásd ebben az értelemben: Tele2 Sverige ítélet (115. pont), valamint Ministerio Fiscal ítélet (55. pont). A Bíróság ezekben az ítéletekben hangsúlyozta a kapcsolatot a beavatkozás súlyossága és az annak igazolása érdekében hivatkozott érdek között.

171 A 29. csoport az elektronikus kommunikáció hírszerzési és nemzetbiztonsági célokból történő megfigyeléséről szóló, 2014. december 5-i munkaanyagában (WP 228, 27. o.) kiemelte, hogy fontos, hogy kritikusan értékeljék, hogy a megfigyelést ténylegesen nemzetbiztonsági célokból végzik-e.

172 Lásd: 1/15 vélemény (181. pont), amelyben a Bíróság kimondta, hogy a beavatkozásokat előíró jogszabályi rendelkezések nem feleltek meg a világosság és az egyértelműség követelményeinek és így nem korlátozódtak a szigorúan szükséges mértékre. Ugyanebből a szempontból Bot főtanácsnok a Schrems ügyre vonatkozó indítványában (C-362/14, EU:C:2015:627, 181–184. pont) úgy ítélte meg, hogy a megfigyelési intézkedések céljait túl általánosan fogalmazták meg ahhoz, hogy azokat a nemzetbiztonság kivételével általános érdekű célnak lehessen tekinteni.

173 Az európai adatvédelmi biztos hasonló kétségeket fejtet ki az EU–USA adatvédelmi pajzs megfelelőségéről szóló határozattervezettel kapcsolatos 2016. május 30-i 4/2016. sz. véleményében (8. o.).

5) A beavatkozások szükségességéről és arányosságáról

290. A Bíróság ismételten kimondta, hogy a Charta 7. és 8. cikkében rögzített jogok nem abszolút jogok, hanem azokat a társadalomban betöltött szerepük függvényében kell vizsgálni, egyúttal az arányosság elvével összhangban biztosítva, hogy egyensúlyban legyenek más alapvető jogokkal.[174] Amint azt a Facebook Ireland kiemelte, e más jogok közé tartozik a Charta 6. cikkében rögzített, biztonsághoz való jog.

291. E tekintetben a szintén állandó ítélkezési gyakorlat szerint a Charta 7. és 8. cikkében biztosított jogokba való bármely beavatkozás esetében szigorú arányossági vizsgálatnak van helye.[175]

292. A Schrems ítéletből így kitűnik, hogy „nem a feltétlenül szükségesre korlátozódik az olyan szabályozás, amely általános jelleggel lehetővé teszi [az] összes személyes [adat]ának tárolását, […] anélkül hogy a kitűzött cél alapján bármilyen különbségtételt, korlátozást vagy kivételt alkalmazna, és anélkül, hogy olyan objektív kritériumot írna elő, amely lehetővé tenné a hatóságok adatokhoz való hozzáférésének és azok későbbi felhasználásának meghatározott célokra történő, szigorúan behatárolt, valamint az ezen adatokhoz való hozzáférés és az azok felhasználása által okozott beavatkozás igazolására alkalmas korlátozását”.[176]

293. A Bíróság azt is kimondta, hogy a kellően indokolt sürgős esetek kivételével a hozzáférésnek előzetes felülvizsgálat tárgyát kell képeznie, amelyet olyan bíróság vagy független közigazgatási szerv végez, amely határozatának célja az adatokhoz való hozzáférésnek és az adatok felhasználásának a követett cél eléréséhez feltétlenül szükséges mértékre történő korlátozása.[177]

294. A GDPR 23. cikkének (2) bekezdése immár egy sor olyan garanciát rögzít, amelyeket a tagállamnak elő kell írnia, amennyiben eltér e rendelet rendelkezéseitől. Az ilyen eltérést lehetővé tévő szabályozásnak tartalmaznia kell többek között az adatkezelés céljaira, az eltérés terjedelmére, a visszaélések megakadályozását célzó garanciákra, az adattárolás időtartamára, valamint az érintettek eltérésről való tájékoztatáshoz való jogára (amennyiben ez nem befolyásolhatja hátrányosan az eltérés célját) vonatkozó rendelkezéseket.

295. A jelen ügyben M. Schrems azt állítja, hogy a FISA 702. cikkéhez nem kapcsolódnak elégséges garanciák az adatokkal való visszaéléssel, illetve a jogosulatlan hozzáféréssel szemben. Közelebbről a kiválasztási tényezők megválasztása nem kellően szabályozott, így e rendelkezés nem nyújt biztosítékokat a közlések tartalmához való általános jellegű hozzáféréssel szemben.

296. Az Egyesült Államok kormánya és a Bizottság ezzel szemben előadja, hogy a FISA 702. cikke objektív kritériumok révén korlátozza a kiválasztási tényezők megválasztását, mivel e rendelkezés az Egyesült Államokon kívül található nem amerikai személyek elektronikus közléseire vonatkozó adatok gyűjtését kizárólag külső hírszerzési információk megszerzése céljából teszi lehetővé.

297. Álláspontom szerint megkérdőjelezhető e kritériumok kellően egyértelmű és pontos jellege, valamint a visszaélés veszélyének elkerülését célzó elégséges garanciák fennállása.

174 Lásd: 2010. november 9-i Volker und Markus Schecke és Eifert ítélet (C-92/09 és C-93/09, EU:C:2010:662, 48. pont); 1/15 vélemény (136. pont); 2019. szeptember 24-i Google ítélet (Linkek közüli törlés területi hatálya) (C-507/17, EU:C:2019:772, 60. pont).

175 Lásd többek között: 2008. december 16-i Satakunnan Markkinapörssi és Satamedia ítélet (C-73/07, EU:C:2008:727, 56. pont); Digital Rights Ireland ítélet (48. és 52. pont); Schrems ítélet (78. és 92. pont); 1/15 vélemény (139. és 140. pont). Lásd még az adatvédelmi pajzsról szóló határozat (140) preambulumbekezdését.

176 Schrems ítélet (93.pont). Lásd még ebben az értelemben: Digital Rights Ireland ítélet (60. pont).

177 Lásd: Tele2 Sverige ítélet (120. pont), valamint 1/15 vélemény (202.pont).

298. Mindenekelőtt az adatvédelmi pajzsról szóló határozat (109) preambulumbekezdésében az szerepel, hogy a kiválasztási tényezőket alkalmazásuk előtt egyedileg nem hagyja jóvá sem a FISC, sem más független bírói vagy közigazgatási szerv. A Bizottság e preambulumbekezdésben azt állapította meg, hogy „a FISC nem egyéni megfigyelési intézkedéseket, hanem megfigyelési programokat […] engedélyez […] éves tanúsítványok alapján”, amit a Bíróság előtt az Egyesült Államok kormánya megerősített. E preambulumbekezdés kimondja, hogy „a FISC által jóváhagyott tanúsítványok nem tartalmaznak információkat a célba vett egyes egyének tekintetében, hanem a [gyűjthető] külföldi hírszerzési információk kategóriáit határozzák meg”. A Bizottság azt is megállapítja, hogy „a FISC nem értékeli – a valószínű ok vagy bármely más standard alapján –, hogy az egyéneket megfelelően veszik-e célba a külföldi hírszerzési információk megszerzéséhez”, noha azt a feltételt ellenőrzi, hogy „az adatszerzés jelentős célja külföldi hírszerzési információk megszerzése[-e]”.

299. Végül az említett preambulumbekezdés szerint a FISA 702. cikke csak akkor engedélyezi az NSA számára a közlések gyűjtését, „ha megalapozottan feltételezhető, hogy az adott kommunikációs eszközt külföldi hírszerzési információk közlésére használják”. Az adatvédelmi pajzsról szóló határozat (70) preambulumbekezdése ehhez hozzáteszi, hogy a kiválasztási tényezők megválasztása a nemzeti hírszerzési prioritási keretben (National Intelligence Priorities Framework, NIPF) történik. E határozat nem tartalmaz a kiválasztási tényezők megválasztása kapcsán pontosabb indokolási vagy igazolási követelményeket az NSA-t kötelező fenti adminisztratív prioritásokra tekintettel. [178]

300. Végül az adatvédelmi pajzsról szóló határozat (71) preambulumbekezdése arra a PPD 28-ban rögzített követelményre utal, amely szerint a külföldi hírszerzési információk gyűjtésének „a lehető legcélzottabbnak kell lennie”. Azonkívül, hogy ez az elnöki irányelv magánszemélyek számára jogokat nem keletkeztet, a „lehető legcélzottabb” tevékenység feltétele és a Charta 52. cikkének (1) bekezdésében a Charta 7. és 8. cikkében garantált jogok gyakorlásába való beavatkozás igazolásához előírt „feltétlen szükségesség” feltétele közötti lényegi azonosság számomra egyáltalán nem tűnik nyilvánvalónak. [179]

301. E megfontolásokra figyelemmel nem biztos, hogy az adatvédelmi pajzsról szóló határozatban ismertetett körülmények alapján a FISA 702. cikkén alapuló megfigyelési intézkedésekhez olyan, a megfigyelési intézkedések esetleges tárgyát képező személyi körre, illetve az adatgyűjtés céljainak korlátozására vonatkozó garanciák kapcsolódnak, amelyek lényegében azonosak a Charta 7. és 8. cikkének fényében értelmezett GDPR által megkövetelt ekkel. [180]

302. Ami egyébként az EO 12333 alapján végzett megfigyeléssel kapcsolatos védelmi szint megfelelőségének értékelését illeti, az EJEB elismeri, hogy a tagállamokat széles mérlegelési mozgástér illeti meg a nemzetbiztonságuk védelmét szolgáló eszközök megválasztása terén, e mozgásteret azonban korlátozza a visszaélésekkel szemben megfelelő és elégséges garanciák előírásának

178 A PCLOB jelentése (45. o.) az alábbiakat tartalmazza: „With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to »identify« the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired. By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence long) that further explains the analyst's rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certification.”

179 Lásd ebben az értelemben: 29. csoport, Opinion 1/2016 on the EU–U. S. Privacy Shield draft adequacy decision, 2016. április 13., WP 238 (3.3.1 pont, 38. o.); az EU–USA adatvédelmi pajzs által nyújtott védelem megfelelőségéről szóló, 2017. április 6-i parlamenti állásfoglalás, P8_TA(2017)0131 (17. pont), valamint a nagy adathalmazok alapjogi vonatkozásairól szóló, 2017. február 20-i parlamenti jelentés: magánélet, adatvédelem, megkülönböztetésmentesség, biztonság és bűnüldözés, A8–0044/2017 (17. pont).

180 Lásd ebben az értelemben: 29. csoport, EU–U. S. Privacy Shield – First Annual Joint Review, 2017. november 28., WP 255 (3. o.); az EU–USA adatvédelmi pajzs által nyújtott védelem megfelelőségéről szóló, 2018. július 5-i parlamenti állásfoglalás, P8_TA(2018)0315 (22. pont), valamint EDPB, EU–U. S. Privacy Shield – Second Annual Joint Review, 2019. január 22. (81–83. és 87. pont).

követelménye.[181] A titkos megfigyelési intézkedésekkel kapcsolatos ítélkezési gyakorlatában az EJEB azt vizsgálja meg, hogy az ezen intézkedések alapját képező belső jog elegendő és tényleges garanciát és korlátot tartalmaz-e ahhoz, hogy teljesüljön az „előreláthatóság” és „a demokratikus társadalomban [való] szükségesség” követelménye.[182]

303. Az EJEB ezzel kapcsolatban rögzít néhány minimális garanciát. E garanciák tárgya azon bűncselekmények természetének megjelölése, amelyek alapján lehallgatás rendelhető el, azon személykategóriák meghatározása, akiknek közlései lehallgathatók, az intézkedés végrehajtási időtartamának korlátozása, a megszerzett adatok vizsgálata, felhasználása és tárolása kapcsán követendő eljárás, az adatok más személyekkel való közlése kapcsán teendő óvintézkedések, valamint azon körülmények, amelyek között a rögzített adatok törlése vagy megsemmisítése megtörténhet, illetve meg kell történnie.[183]

304. A beavatkozással kapcsolatos garanciák megfelelő és tényleges jellege az ügy valamennyi körülményének függvénye, beleértve az intézkedések jellegét, terjedelmét és időtartamát, az elrendelésükhöz szükséges indokokat, az intézkedések lehetővé tételére, végrehajtására és ellenőrzésére hatáskörrel rendelkező hatóságokat, valamint a belső jog által biztosított jogorvoslat típusát.[184]

305. Közelebbről, egy titkos megfigyelési intézkedés igazolásának értékelése során az EJEB a megfigyelés „elrendelésekor”, „lefolytatása során” és „befejeződése után” végzett valamennyi ellenőrzést figyelembe veszi.[185] Az említett három szakasz közül az elsővel kapcsolatban az EJEB azt követeli meg, hogy az ilyen intézkedést független szerv engedélyezze. Noha álláspontja szerint a bírói hatalmi ág biztosítja a függetlenség, pártatlanság és megfelelő eljárás legjobb garanciáit, a szóban forgó szervnek nem kell feltétlenül a bírósági szervezethez tartoznia.[186] A későbbi szakaszokban folytatott alapos bírósági felülvizsgálat ellensúlyozhatja az engedélyezési eljárás esetleges hiányosságait.[187]

306. A jelen esetben az adatvédelmi pajzsról szóló határozatból kitűnik, hogy kizárólag az adatok Egyesült Államok területén kívüli gyűjtését és felhasználását korlátozó garanciák szerepelnek a PPD 28-ban, mivel a FISA 702. cikke nem alkalmazandó e területen kívül. Nem vagyok meggyőződve arról, hogy e garanciák elegendőek lehetnek az „előreláthatóság” és „a demokratikus társadalomban [való] szükségesség” követelményének teljesüléséhez.

307. Először is már rámutattam, hogy ez az elnöki irányelv magánszemélyek számára jogokat nem keletkeztet. Ezt követően, kétlem, hogy a „lehető legcélzottabb” megfigyelés biztosításának követelménye kellően egyértelműen és pontosan van megfogalmazva ahhoz, hogy megfelelő védelmet biztosítson az érintettek számára a visszaélés veszélyével szemben.[188] Végül az adatvédelmi pajzsról szóló határozat nem állapítja meg azt, hogy az EO 12333-on alapuló megfigyelést utólag független szerv felülvizsgálja, vagy hogy az utólagos bírósági felülvizsgálat tárgya lehet.[189]

181 Lásd többek között: Zakharov ítélet (232. §), valamint Szabó és Vissy ítélet (57. §).

182 Lásd többek között: Zakharov ítélet (237. §); Centrüm för Rättvisa ítélet (111. §), valamint Big Brother Watch ítélet (322. §).

183 Lásd többek között: Weber és Saravia határozat (95. §); EJEB, 2007. június 28., Association pour l’intégration européenne et les droits de l’homme és Ekimdjiev (CE:ECHR:2007:0628JUD006254000, 76. §), valamint Zakharov ítélet (231. §).

184 Lásd többek között: Weber és Saravia határozat (106. §); Zakharov ítélet (232. §), valamint Centrüm för Rättvisa ítélet (104. §).

185 Lásd többek között: EJEB, 1978. szeptember 6., Klass és társai kontra Németország (CE:ECHR:1978:0906JUD000502971, 55. §); Zakharov ítélet (233. §), valamint Centrüm för Rättvisa ítélet (105. §).

186 Lásd többek között: Klass ítélet (56. §); EJEB, 2010. május 18., Kennedy kontra Egyesült Királyság ítélet (CE:ECHR:2010:0518JUD002683905, 167. §), valamint Zakharov ítélet (233. és 258. §).

187 Lásd: Szabó és Vissy ítélet (77. §), valamint Centrüm för Rättvisa ítélet (133. §).

188 Még inkább ez a helyzet a jelen indítvány 281. pontjában kifejtett megfontolásokra figyelemmel.

189 Lásd a jelen indítvány 330. és 331. pontját.

308. E körülmények között kérdéses számomra azon megállapítás megalapozottsága, amely szerint az Egyesült Államok, hírszerző szolgálatainak a FISA 702. cikkének, valamint az EO 12333-on alapuló tevékenységei során a GDPR 45. cikkének a Charta 7. és 8. cikkének, illetve az EJEE 8. cikkének fényében értelmezett (1) bekezdése értelmében vett megfelelő szintű védelmet biztosít.

c) Az adatvédelmi pajzsról szóló határozat érvényességéről a hatékony jogorvoslathoz való jog szempontjából

309. Az előzetes döntéshozatalra előterjesztett ötödik kérdés annak eldöntésére hívja fel a Bíróságot, hogy azon személyek, akiknek adatait az Egyesült Államokba továbbítják, ott lényegében azonos védelmet élveznek-e, mint amelyet a Charta 47. cikke alapján az Unióban kell biztosítani. Tizedik kérdésével a kérdést előterjesztő bíróság lényegében azt kérdezi a Bíróságtól, hogy az ötödik kérdésre igenlő választ kell-e adni, figyelemmel arra, hogy az adatvédelmi pajzsról szóló határozat bevezette a közvetítési mechanizmust.

310. Kiindulásként megállapítom, hogy a Bizottság e határozat (115) preambulumbekezdésében elismeri, hogy az amerikai jogrendszer az egyének bírói jogvédelmét illetően hiányosságokkal rendelkezik.

311. E preambulumbekezdés szerint először is a bírói jogorvoslati lehetőségek „nem terjednek ki legalább néhány olyan jogalapra (pl. az [EO 12333-ra]), amelyet az Egyesült Államok hírszerzési hatóságai igénybe vehetnek”. Az EO 12333 és a PPD 28 ugyanis nem keletkeztetnek jogokat az érintettek számára és azokra nem lehet hivatkozni bíróság előtt. Márpedig a hatékony bírói jogvédelem feltételezi legalább azt, hogy a magánszemélyek bíróság előtt hivatkozható jogokkal rendelkeznek.

312. Másodszor, „még ha elvben léteznek is bírósági jogorvoslati lehetőségek a nem amerikai személyek számára, például a FISA alapján végzett megfigyelés esetében, a rendelkezésre álló kereseti jogcímek korlátozottak, és [a] kereseteket elfogadhatatlannak nyilvánítják, amennyiben nem tudnak olyan »perképességet« igazolni, amely korlátozza a rendes bíróságokhoz fordulást”.

313. Az adatvédelmi pajzsról szóló határozat (116)–(124) preambulumbekezdéséből kitűnik, hogy az ombudsman intézménye korlátozások kompenzálását célozza. A Bizottság e határozat (139) preambulumbekezdésében megállapítja, hogy „az adatvédelmi pajzs által előírt *felügyeleti* és *jogorvoslati* mechanizmusok *összességében véve* […] jogorvoslatok[at] [biztosítanak] az érintetteknek ahhoz, hogy betekinthessenek a rájuk vonatkozó személyes adatokba, és esetleg helyesbítsék vagy töröljék ezeket az adatokat” (kiemelés tőlem).

314. Felidézve a Bíróság és az EJEB közlések megfigyelésére vonatkozó intézkedésekkel kapcsolatos ítélkezési gyakorlatából következő elveket, a továbbiakban megvizsgálom, hogy az amerikai jog által előírt, az adatvédelmi pajzsról szóló határozatban ismertetett bírói jogorvoslatok lehetővé teszik-e az érintettek megfelelő bírói jogvédelmének biztosítását (1. rész). Ezt követően megvizsgálom, hogy a közvetítés bíróságon kívüli mechanizmusának bevezetése lehetővé teszi-e adott esetben az e személyek bírói jogvédelmét jellemző esetleges hiányosságok kompenzálását (2. rész).

1) Az amerikai jogban előírt bírói jogorvoslatok hatékonyságáról

315. A Charta 47. cikkének első bekezdése értelmében mindenkinek, akinek az Unió joga által biztosított jogait és szabadságait megsértették, joga van a bíróság előtti hatékony jogorvoslathoz.[190] E cikk második bekezdése szerint mindenkinek joga van arra, hogy ügyét független és pártatlan bíróság tárgyalja.[191] A független bírósághoz való hozzáférés a Charta 47. cikkében garantált jog lényeges tartalmához tartozik.[192]

316. Ez az egyéni bírói jogvédelemhez való jog ahhoz a tagállamokat a Charta 7. és 8. cikke alapján terhelő kötelezettséghez kapcsolódik, hogy kellően indokolt sürgős esetek kivételével minden megfigyelési intézkedést előzetesen felül kell vizsgálnia egy bíróságnak vagy egy független közigazgatási hatóságnak.[193]

317. Nem vitás, amint azt a német és a francia kormány is kifejti, hogy a hatékony bírósági jogorvoslathoz való jog nem jelent abszolút garanciát,[194] mivel e jog nemzetbiztonsági okokból korlátozható. Eltérések azonban csak akkor megengedettek, ha azok nem sértik e jog lényeges tartalmát és feltétlenül szükségesek valamely jogszerű cél eléréséhez.

318. E tekintetben a Bíróság a Schrems ítéletben kimondta, hogy az olyan szabályozás, amely nem biztosít a jogalany számára *semmilyen jogorvoslati lehetőséget* abból a célból, hogy a rá vonatkozó személyes adatokhoz hozzáférést kapjon, vagy azokat helyesbíttesse, illetve töröltesse, nem tartja tiszteletben a Charta 47. cikkében szereplő alapvető jogot.[195]

319. Hangsúlyozom, hogy e hozzáférési jog magával vonja annak lehetőségét, hogy jogszerű érdekének érvényesítéséhez szigorúan szükséges eltérések kivételével valamely személy *visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e*.[196] Álláspontom szerint ez a gyakorlati tartalma a hozzáférési jognak, amennyiben az érdekelt személy nem tudja, hogy a hatóságok tároltak-e vele kapcsolatos személyes adatokat többek között az elektronikus kommunikációáramlások automatikus szűrését szolgáló eljárás eredményeként.

190 A Chartához fűzött magyarázatok e tekintetben kifejtik, hogy „[a]z uniós jogban [a Charta 47. cikke által biztosított] védelem szélesebb körű, [mint az EJEE 13. cikke által előírt,] mivel bíróság előtti hatékony jogorvoslathoz való jogot biztosít". Lásd még: Wathelet főtanácsnok Berlioz Investment Fund ügyre vonatkozó indítványa (C-682/15, EU:C:2017:2, 37. pont).

191 A Charta 47. cikke alapján valamely szerv „bírósági" minőségének értékelése céljából figyelembe kell venni azt, hogy e szerv jogszabály alapján jött-e létre, állandó jelleggel működik-e, hatásköre kötelező jellegű-e, az eljárása kontradiktórius jellegű-e, jogszabályokat alkalmaz-e, valamint hogy független-e. Lásd: 2018. február 27-i Associação Sindical dos Juízes Portugueses ítélet (C-64/16, EU:C:2018:117, 38. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

192 Lásd többek között: 2018. július 25-i Minister for Justice and Equality (Az igazságszolgáltatási rendszer hiányosságai) (C-216/18 PPU, EU:C:2018:586, 59. és 63. pont); 2019. november 5-i Bizottság kontra Lengyelország ítélet (A rendes bíróságok függetlensége) (C-192/18, EU:C:2019:924, 106. pont); 2019. november 19-i A. K. és társai ítélet (A legfelsőbb bíróság fegyelmi tanácsának függetlensége) (C-585/18, C-624/18 és C-625/18, EU:C:2019:982, 120. pont).

193 Lásd a jelen indítvány 293. pontját. A GDPR 45. cikke (3) bekezdésének a) pontja azt írja elő, hogy a harmadik ország által nyújtott védelmi szint megfelelőségének mérlegelése során figyelembe kell venni az érintettek által hatékonyan érvényesíthető „hatékony közigazgatási és bírósági jogorvoslatot" (kiemelés tőlem). Ugyanígy, a GDPR (104) preambulumbekezdése szerint a megfelelőségi határozat feltételeként meg kell követelni, hogy az adott harmadik országban az érintettek „hatékony közigazgatási és bírósági jogorvoslati lehetőségekkel" rendelkezzenek (kiemelés tőlem). Lásd még: 29. csoport, EU–U. S. Privacy Shield – First Annual Joint Review, 2017. november 28., WP 255 (B. 3. pont); az EU–USA adatvédelmi pajzs által nyújtott védelem megfelelőségéről szóló, 2018. július 5-i parlamenti állásfoglalás, P8_TA(2018)0315 (25. és 30. pont), valamint EDPB, EU–U. S. Privacy Shield – Second Annual Joint Review, 2019. január 22. (94–97. pont).

194 Lásd ebben az értelemben: 2013. február 28-i Arango Jaramillo és társai kontra EBB ítélet (felülvizsgálat), (C-334/12 RX-II, EU:C:2013:134, 43. pont).

195 Schrems ítélet (95. pont).

196 A GDPR „Az érintett hozzáférési joga" című 15. cikkének (1) bekezdése szerint e személy „jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz […] hozzáférést kapjon". Az adatvédelmi pajzsról szóló határozat II. melléklete II. 8. pontjának a) alpontjában előírt „hozzáférési elv" jelentése ugyanez.

320. Egyébként az ítélkezési gyakorlatból kitűnik, hogy a tagállami hatóságok főszabály szerint kötelesek tájékoztatást adni az adatokhoz való hozzáférésről, *amikor e tájékoztatás már nem veszélyeztetheti a folyamatban levő nyomozást.*[197] E tájékoztatás ugyanis előfeltétele a Charta 47. cikkében rögzített jogorvoslathoz való jognak.[198] E kötelezettség immár a GDPR 23. cikke (2) bekezdésének h) pontjában is szerepel.

321. Az adatvédelmi pajzsról szóló határozat (111)–(135) preambulumbekezdése röviden ismerteti az azon személyek rendelkezésére álló valamennyi jogorvoslati lehetőséget, akiknek adatait továbbították, amennyiben attól tartanak, hogy ezeket az adatokat az amerikai hírszerző szolgálatok az adattovábbítást követően felhasználták. E jogorvoslati lehetőségeket a High Court (felsőbíróság) 2017. október 3-i ítélete, valamint többek között az Egyesült Államok kormányának észrevételei is ismertetik.

322. Ezen észrevételek tartalmát nem szükséges részletesen felidézni. A kérdést előterjesztő bíróság ugyanis az érintettek jogvédelmére vonatkozó garanciák megfelelőségét lényegében azzal az indokkal kérdőjelezi meg, hogy a kereshetőségi joggal (*standing*) kapcsolatos különösen szigorú követelmények,[199] a megfigyelési intézkedés tárgyát képező személyek tájékoztatására vonatkozó bármely kötelezettség nélkül, *még akkor is, ha a tájékoztatás már nem veszélyeztetné a célokat*, a gyakorlatban túlzottan nehézzé tennék az Egyesült Államok jogában előírt jogorvoslati lehetőségek gyakorlását. E kétségeket osztja a DPC, M. Schrems, az osztrák, a lengyel és a portugál kormány, valamint az EDPB.[200]

323. Ezzel kapcsolatban annak felidézésére szorítkozom, hogy a kereshetőségi joggal kapcsolatos szabályok nem sérthetik a hatékony bírói jogvédelmet,[201] valamint megállapítom, hogy az adatvédelmi pajzsról szóló határozat egyáltalán nem utal az érintettek arról való tájékoztatásával kapcsolatos követelményre, hogy megfigyelési intézkedés tárgyát képezték.[202] Mivel alkalmas lehet a bírósági jogorvoslati lehetőségek érvényesítésének megakadályozására, az ilyen intézkedésről való tájékoztatásra irányuló kötelezettség hiánya, még abban az esetben is, ha az érintett értesítése immár nem ártana az intézkedés hatékonyságának, problematikusnak tűnik a jelen indítvány fenti 320. pontjában hivatkozott ítélkezési gyakorlatra figyelemmel.

324. Az adatvédelmi pajzsról szóló határozat 169. lábjegyzete ezenkívül elismeri, hogy a rendelkezésre álló kereseti jogcímek „megkövetelik a kár megvalósulását […] vagy annak igazolását, hogy […] a kormány fel kívánja használni vagy nyilvánosságra szándékozik hozni azokat az információkat, amelyeket az érintett személy elektronikus megfigyelésével szereztek”. Amint azt a kérdést előterjesztő

197 Tele2 Sverige ítélet (121. pont), valamint 1/15 vélemény (220. pont). Amint azt a Facebook Ireland megjegyzi, a hatóságok adatokhoz való hozzáféréséről szóló tájékoztatás tehát nem követelhető meg rendszerszerűen. Ennek kapcsán az EJEB úgy véli, hogy „[a] gyakorlatban elképzelhető, hogy nem lehet utólagos tájékoztatást előírni”, mivel a megfigyelési intézkedések tárgyát képező fenyegetés „évekig, sőt évtizedekig fennállhat” ezen intézkedések megszüntetését követően, így a tájékoztatás „veszélyeztetheti a megfigyelést eredetileg indokolttá tévő hosszú távú célt”, valamint „felfedheti a hírszerző szolgálatok munkamódszereit, tevékenységi körüket és […] ügynökeik személyét” (Zakharov ítélet [287. §], valamint az ott hivatkozott ítélkezési gyakorlat). Tájékoztatás hiányában, noha a jogszabályi előírások megsértése esetén az egyéni jogorvoslati lehetőségek ebből következően nem gyakorolhatók, más garanciák elegendőek lehetnek a magánélet tiszteletben tartásához való jog megvédéséhez (lásd még a Centrüm för Rättvisa ítéletet, 164–167. és 171–178. §). Lásd a jelen indítvány 330. pontját.

198 Lásd e tekintetben a jelen indítvány 210. pontját.

199 Lásd a jelen indítvány 67. pontját.

200 Lásd: EDPB, EU-U. S. Privacy Shield – Second Annual Joint Review, 2019. január 22. (18. o., 97. pont).

201 Lásd többek között: 1991. július 11-i Verholan és társai ítélet (C-87/90–C-89/90, EU:C:1991:314, 24. pont, valamint az ott hivatkozott ítélkezési gyakorlat), továbbá 2013. február 28-i Arango Jaramillo és társai kontra EBB ítélet (felülvizsgálat), C-334/12 RX-II, EU:C:2013:134, 43. pont).

202 Az Egyesült Államok kormánya ugyanakkor a kérdést előterjesztő bírósághoz hasonlóan kiemelte, hogy a FISA 702. cikken alapuló megfigyelési intézkedésről tájékoztatni kell a célszemélyt, amennyiben a gyűjtött adatokat bírósági eljárás során felhasználják ellene.

bíróság, a DPC és M. Schrems hangsúlyozta, e követelmény ellentétben áll a Bíróság azon ítélkezési gyakorlatával, amely szerint az érintett magánélet tiszteletben tartásához való alapvető jogába történő beavatkozás megállapítása érdekében nem szükséges, hogy az érintetteknek az állítólagos beavatkozás esetleges kellemetlenséget okozzon. [203]

325. Egyébként számomra nem meggyőző a Facebook Ireland és az Egyesült Államok kormánya által kifejtett álláspont, amely szerint az azon személyek bírói jogvédelmét jellemző hiányosságokat, akiknek adatait az Egyesült Államokba továbbították, kompenzálják a FISC által végzett előzetes és utólagos ellenőrzések, valamint a végrehajtó hatalom és a jogalkotó hatalom keretében kialakított több felügyeleti mechanizmus. [204]

326. Már rámutattam, hogy egyrészt az adatvédelmi pajzsról szóló határozatban szereplő megállapításoknak megfelelően a FISC nem ellenőrzi az egyéni megfigyelési intézkedéseket azok végrehajtását megelőzően. [205] Másrészt, amint az e határozat (109) preambulumbekezdésében szerepel, és amint azt az Egyesült Államok kormánya a Bíróság kérdéseire adott írásbeli válaszában megerősítette, a kiválasztási tényezők alkalmazását érintő utólagos ellenőrzés célja a kiválasztási tényezők megválasztását szabályozó, az éves tanúsításokban előírt feltételek tiszteletben tartásának ellenőrzése, amennyiben valamely hírszerző ügynökség a személyre irányultságra és az adattakarékosságra vonatkozó eljárások esetleges megsértésével kapcsolatos eseményre hívta fel a FISC figyelmét. [206] A FISC előtti eljárás tehát láthatóan nem biztosít tényleges egyéni jogorvoslati lehetőséget azon személyek számára, akiknek adatait az Egyesült Államokba továbbítják.

327. Az adatvédelmi pajzsról szóló határozat (95)–(110) preambulumbekezdésében említett ellenőrzési mechanizmusok, noha adott esetben megerősíthetik az esetleges bírósági jogorvoslati lehetőségeket, álláspontom szerint nem lehetnek elegendőek ahhoz, hogy megfelelő védelmi szintet biztosítsanak az érintett személyek jogorvoslathoz való joga tekintetében. Közelebbről az egyes ügynökségek belső szervezetéhez tartozó főellenőrök véleményem szerint nem minősülnek független ellenőrzési mechanizmusnak. A PCLOB és a Kongresszus hírszerzési bizottságai által gyakorolt felügyelet nem egyenértékű a megfigyelési intézkedésekkel szemben egyéni jogorvoslati mechanizmussal.

328. Ennélfogva meg kell vizsgálni, hogy az ombudsman intézménye orvosolja-e ezeket a hiányosságokat, hatékony jogorvoslati lehetőséget biztosítva az érintettek számára egy független és pártatlan szerv előtt. [207]

329. Másodszor, emlékeztetek arra, hogy az adatvédelmi pajzsról szóló határozatban szereplő megfelelőségi megállapítás megalapozottságának az azon személyek rendelkezésére álló jogorvoslati lehetőségekre tekintettel történő értékelése szempontjából, akik úgy vélik, hogy az EO 12333 alapján megfigyelték őket, a releváns viszonyítási alapot az EJEE rendelkezései jelentik.

203 2003. május 20-i Österreichischer Rundfunk és társai ítélet (C-465/00, C-138/01 és C-139/01, EU:C:2003:294, 75. pont); Digital Rights Ireland ítélet (33. pont); Schrems ítélet (87. pont); 1/15 vélemény (124. pont).

204 E mechanizmusokat az adatvédelmi pajzsról szóló határozat (95)–(110) preambulumbekezdése ismerteti. A Bizottság ezekben a rendelkezésekben a „hatékony jogvédelemre” vonatkozó szabályok kategóriáján belül megkülönbözteti a felügyeleti mechanizmusokat (lásd a (92–(110) preambulumbekezdést) és az egyéni jogorvoslatokat (lásd a (111)–(124) preambulumbekezdést).

205 Lásd a jelen indítvány 298. pontját.

206 Az adatvédelmi pajzsról szóló határozat (109) preambulumbekezdése szerint „[a] legfőbb ügyész és [az NSA] igazgatója ellenőrzi a megfelelést és az ügynökségek kötelesek bármely megfelelés hiányára utaló eseményt bejelenteni a FISC-nek […], amely ennek alapján módosíthatja az engedélyezést”.

207 Lásd a jelen indítvány 333–340. pontját.

330. Amint azt korábban kifejtettem,[208] annak értékelése során, hogy egy megfigyelési intézkedés megfelel-e az „előreláthatóság” és az EJEE 8. cikke (2) bekezdésének értelmében vett „a demokratikus társadalomban szükségesség” követelményének,[209] az EJEB összességükben vizsgálja az intézkedést „megelőzően, az alatt és azt követően” érvényesített ellenőrzési és felügyeleti mechanizmusokat. Amennyiben az egyéni jogorvoslat érvényesítésének akadályát az jelenti, hogy a megfigyelési intézkedésről való tájékoztatás csak az intézkedés hatékonyságának veszélyeztetésével tehető meg,[210] e hiányosságot ellensúlyozhatja a szóban forgó intézkedés alkalmazását megelőzően végrehajtott független ellenőrzés.[211] Ily módon az EJEB, noha úgy véli, hogy e tájékoztatás „kívánatos”, amennyiben arra a megfigyelési intézkedés hatékonyságának lerontása nélkül sor kerülhet, ezt nem fogalmazta meg követelményként.[212]

331. E tekintetben az adatvédelmi pajzsról szóló határozatból nem tűnik ki, hogy az EO 12333-on alapuló megfigyelési intézkedésekről tájékoztatnák az érintetteket, illetve hogy azokhoz elfogadásuk vagy végrehajtásuk bármely szakaszában független bírósági vagy közigazgatási felülvizsgálati mechanizmusok kapcsolódnának.

332. E körülmények között azt kell megvizsgálni, hogy az ombudsmanhoz fordulás mindazonáltal lehetővé teszi-e a megfigyelési intézkedések független ellenőrzését, abban az esetben is, ha azok az EO 12333-on alapulnak.

2) A közvetítési mechanizmus hatékony jogorvoslathoz való jog szintjére gyakorolt hatásáról

333. Az adatvédelmi pajzsról szóló határozat (116) preambulumbekezdése szerint az e határozat III. A. mellékletében ismertetett közvetítési mechanizmus célja az, hogy további jogorvoslati lehetőséget biztosítson minden olyan személy számára, akinek adatait az Európai Unióból az Egyesült Államokba továbbították.

334. Amint azt az Egyesült Államok kormánya kiemelte, az ombudsmanhoz benyújtott panasz elfogadhatóságának nem feltétele az amerikai bíróságokhoz fordulást szabályozókhoz hasonló, a kereshetőségi jogra vonatkozó szabályok tiszteletben tartása. Az említett határozat (119) preambulumbekezdése ezzel kapcsolatban kimondja, hogy az ombudsmanhoz fordulásnak nem feltétele, hogy az érintett bizonyítsa, hogy az Egyesült Államok kormánya betekintett a rá vonatkozó adatokba.

335. A DPC-hez, M. Schrems-hez, a lengyel és a portugál kormányhoz, valamint az EPIC-hez hasonlóan kétségeim vannak azzal kapcsolatban, hogy e mechanizmus képes-e kompenzálni az azon személyek részére nyújtott bírói védelem hiányosságait, akiknek adatait az Európai Unióból az Egyesült Államokba továbbították.

208 Lásd a jelen indítvány 305. pontját.

209 A távközlés megfigyelését szolgáló intézkedésekkel kapcsolatos ítélkezési gyakorlatában az EJEB a jogorvoslati lehetőségek kérdésére a „törvényi minőség” és az EJEE 8. cikkében garantált jog gyakorlásába való beavatkozás szükségességének vizsgálata során tért ki (lásd többek között: Zakharov ítélet [236. §] és Centrüm för Rättvisa ítélet [107. §]). Az EJEB a 2008. július 1-jei Liberty és társai kontra Egyesült Királyság ítéletben (CE:ECHR:2008:0701JUD005824300, 73.) és a Zakharov ítéletben (307. §), miután megállapította az EJEE 8. cikkének megsértését, nem tartotta szükségesnek az ezen egyezmény 13. cikkére alapított jogalap külön vizsgálatát.

210 Az EJEB szerint, noha a tájékoztatás elmaradása egyik szakaszban sem jelenti szükségképpen akadályát annak, hogy a megfigyelési intézkedés megfeleljen „a demokratikus társadalomban szükségesség” feltételének, az veszélyezteti a bíróságokhoz való hozzáférést és ebből következően a jogorvoslatok tényleges érvényesülését (lásd többek között: 1978. szeptember 6., Klass és társai kontra Németország [CE:ECHR:1978:0906JUD000502971, 57. és 58. §]; Weber és Saravia határozat [135. §]; Zakharov ítélet [302. §]).

211 Lásd ebben az értelemben: Centrum för Rättvisa ítélet (105. §).

212 A Big Brother Watch ítéletben (317. §) az EJEB megtagadta az érintett személyek megfigyelésről való tájékoztatására vonatkozó követelmény beiktatását az elektronikus közlések tömeges megfigyelésével járó megfigyelési szabályozásra alkalmazandó minimális garanciák közé. Lásd még: Centrum för Rättvisa ítélet (164. §). Annak, hogy ezen ítéleteket az EJEB Nagykamarája elé utalták, többek között e következtetés felülvizsgálata volt a célja.

336. Mindenekelőtt, noha egy bíróságon kívüli jogorvoslati mechanizmus az EUMSZ 47. cikk értelmében vett hatékony jogorvoslatnak minősülhet, ez különösen csak akkor áll fenn, ha a szóban forgó szerv jogszabály alapján jött-e létre és megfelel a függetlenség követelményének.[213]

337. Márpedig az adatvédelmi pajzsról szóló határozatból kitűnik, hogy a PPD 28-on alapuló közvetítési mechanizmus[214] nem jogszabály alapján jött létre. Az ombudsmant a külügyminiszter nevezi ki és szerves részét képezi az Egyesült Államok külügyminisztériumának.[215] E határozat egyáltalán nem utal arra, hogy az ombudsman visszahívásához vagy kinevezésének megszüntetéséhez bármilyen különös garancia kapcsolódna.[216] Noha az ombudsmant úgy írják le, hogy az független a „hírszerző szervezetektől", a külügyminiszter felé felel, ennélfogva nem független a végrehajtó hatalomtól.[217]

338. Ezt követően, a bíróságon kívüli jogorvoslati lehetőség hatékonysága álláspontom szerint a szóban forgó szerv azon képességétől is függ, hogy kötelező és indokolt határozatokat fogadjon el. E kérdést illetően az adatvédelmi pajzsról szóló határozat semmilyen utalást nem tartalmaz arra vonatkozóan, hogy az ombudsman ilyen határozatokat hozna. Nem rögzíti, hogy az ombudsman intézménye lehetővé teszi a kérelmezők számára a hozzáférést a rájuk vonatkozó adatokhoz, illetve azok kijavítását vagy törlését, továbbá az ombudsman nem ítél meg kártérítést a megfigyelési intézkedés által sértett személyek számára. Közelebbről, amint az e határozat III. A. melléklete 4. pontjának e) alpontjából kitűnik, „[az] ombudsman nem erősíti meg és nem is cáfolja, hogy az egyén megfigyelés célpontja volt, és […] nem erősíti meg az alkalmazott konkrét jogorvoslatot".[218] Noha az amerikai kormány kötelezettséget vállalt arra, hogy a hírszerzés érintett szervezetének orvosolnia kell az alkalmazandó szabályok ombudsman által felderített bármely megsértését,[219] az említett határozat nem rögzít az e kötelezettségvállaláshoz kapcsolódó olyan jogszabályi garanciákat, amelyekre az érintett egyének hivatkozhatnának.

339. Következésképpen az ombudsman intézménye álláspontom szerint nem nyújt olyan független szerv előtti jogorvoslati lehetőséget, amely lehetőséget kínál azon személyek számára, akiknek adatait továbbították, arra, hogy az adatokhoz való hozzáféréshez való jogukra hivatkozzanak, vagy kifogásolják a hírszerző szolgálatokra alkalmazandó szabályok megsértését.

213 A függetlenség fogalmának van egy első, külső vonatkozása, amely azt feltételezi, hogy az érintett szerv védve van az olyan külső beavatkozástól vagy nyomástól, amely veszélyeztetheti tagjai ítéletalkotásának függetlenségét az eléjük kerülő jogvitákat illetően. A második, belső vonatkozás a „pártatlanság" fogalmával áll összefüggésben, és arra vonatkozik, hogy egyenlő távolságot kell tartani a jogvitában részt vevő felektől, illetve e feleknek a jogvita tárgyához fűződő mindenkori érdekeitől. Lásd többek között: 2006. szeptember 19-i Wilson ítélet (C-506/04, EU:C:2006:587, 50–52. pont); 2018. július 25-i Minister for Justice and Equality (Az igazságszolgáltatási rendszer hiányosságai) (C-216/18 PPU, EU:C:2018:586, 63. és 65. pont); 2019. november 19-i A. K. és társai ítélet (A legfelsőbb bíróság fegyelmi tanácsának függetlensége) (C-585/18, C-624/18 és C-625/18, EU:C:2019:982, 121. és 122. pont). A hatalmi ágak elválasztása elvének megfelelően a bíróságok függetlenségét a jogalkotó és a végrehajtó hatalommal szemben kell biztosítani. Lásd: 2019. november 19-i A. K. és társai ítélet (A legfelsőbb bíróság fegyelmi tanácsának függetlensége) (C-585/18, C-624/18 és C-625/18, EU:C:2019:982, 127. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

214 Az adatvédelmi pajzsról szóló határozat III. A. melléklete e tekintetben a PPD 28 4. szakaszának d) pontjára utal.

215 Lásd az adatvédelmi pajzsról szóló határozat (116) preambulumbekezdését.

216 A 2005. május 31-i Syfait és társai ítéletben (C-53/03, EU:C:2005:333, 31. pont) a Bíróság hangsúlyozta az ilyen garanciák fontosságát a függetlenség követelményének teljesülése szempontjából. Lásd még e tekintetben: 2019. június 24-i Bizottság kontra Lengyelország ítélet (A legfelsőbb bíróság függetlensége), (C-619/18, EU:C:2019:531, 76. pont); 2019. november 5-i Bizottság kontra Lengyelország ítélet (A rendes bíróságok függetlensége) (C-192/18, EU:C:2019:924, 113. pont).

217 Lásd az adatvédelmi pajzsról szóló határozat (65) és (121) preambulumbekezdését, valamint III. A. mellékletének 1. pontját.

218 Ezenkívül az adatvédelmi pajzsról szóló határozat (121) preambulumbekezdésében az szerepel, hogy „az ombudsmannak kell megerősítenie, hogy i. a panaszt megfelelően kivizsgálták, valamint ii. betartották a vonatkozó amerikai jogot – így különösen a VI. mellékletben ismertetett korlátozásokat és biztosítékokat –, vagy a megfelelés hiánya esetén orvosolták ezt a jogsértést".

219 A Bizottság az adatvédelmi pajzs harmadik éves felülvizsgálata során megállapította, hogy az Egyesült Államok kormányának nyilatkozatai alapján abban az esetben, ha az ombudsman vizsgálata a személyre irányultságra és az adattakarékosságra vonatkozó, a FISC által jóváhagyott eljárások megsértését állapítja meg, erről tájékoztatnia kell e bíróságot. A FISC ilyenkor független vizsgálatot folytat és szükség esetén kötelezi az érintett hírszerző szervet az említett jogsértés orvoslására. Lásd: Commission staff working document accompanying the report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U. S. Privacy Shield, 2019. október 23., SWD(2019) 390 végleges, 28. o. A Bizottság a „Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure" című, az alábbi címen elérhető dokumentumra hivatkozik:
https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf (4. és 5. o.).

340. Végül az ítélkezési gyakorlatnak megfelelően a Charta 47. cikkében biztosított jog tiszteletben tartása feltételezi, hogy ha e közigazgatási hatóság határozata maga nem felel meg a függetlenség és pártatlanság feltételeinek, az később olyan bíróság felülvizsgálatának tárgya lehet, amely hatáskörrel rendelkezik valamennyi releváns kérdés eldöntésére.[220] Ugyanakkor az adatvédelmi pajzsról szóló határozatban szereplő adatok szerint az ombudsman határozatait független bíróság nem vizsgálja felül.

341. E körülmények között, amint azt a DPC, M. Schrems, az EPIC, valamint a lengyel és a portugál kormány kifejti, az Egyesült Államok jogrendjében azon személyek számára biztosított bírói jogvédelem, akiknek adatait az Unióból ebbe az országba továbbították, valamint a Charta 47. cikkének és az EJEE 8. cikkének fényében értelmezett GDPR-ből következő védelem közötti lényegi azonosság álláspontom szerint kérdéses.

342. A fenti megfontolások összességére figyelemmel bizonyos kétségeim vannak azzal kapcsolatban, hogy az adatvédelmi pajzsról szóló határozat megfelel-e a GDPR 45. cikke – Charta 7., 8. és 47. cikkének, valamint az EJEE 8. cikkének fényében értelmezett – (1) bekezdésének.

V. Végkövetkeztetés

343. Azt javaslom a Bíróságnak, hogy a High Court (felsőbíróság, Írország) által előzetes döntéshozatal céljából feltett kérdésekre a következőképpen válaszoljon:

Az előzetes döntéshozatalra előterjesztett kérdések elemzése nem tárt fel olyan körülményt, amely kihatna a 2016. december 16-i (EU) 2016/2297 bizottsági végrehajtási határozattal módosított, a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló, 2010. február 5-i 2010/87/EU bizottság határozat érvényességére.

220 Lásd: 2017. május 16-i Berlioz Investment Fund ítélet (C-682/15, EU:C:2017:373, 55. pont); 2017. december 13-i El Hassani ítélet (C-403/16, EU:C:2017:960, 39. pont).